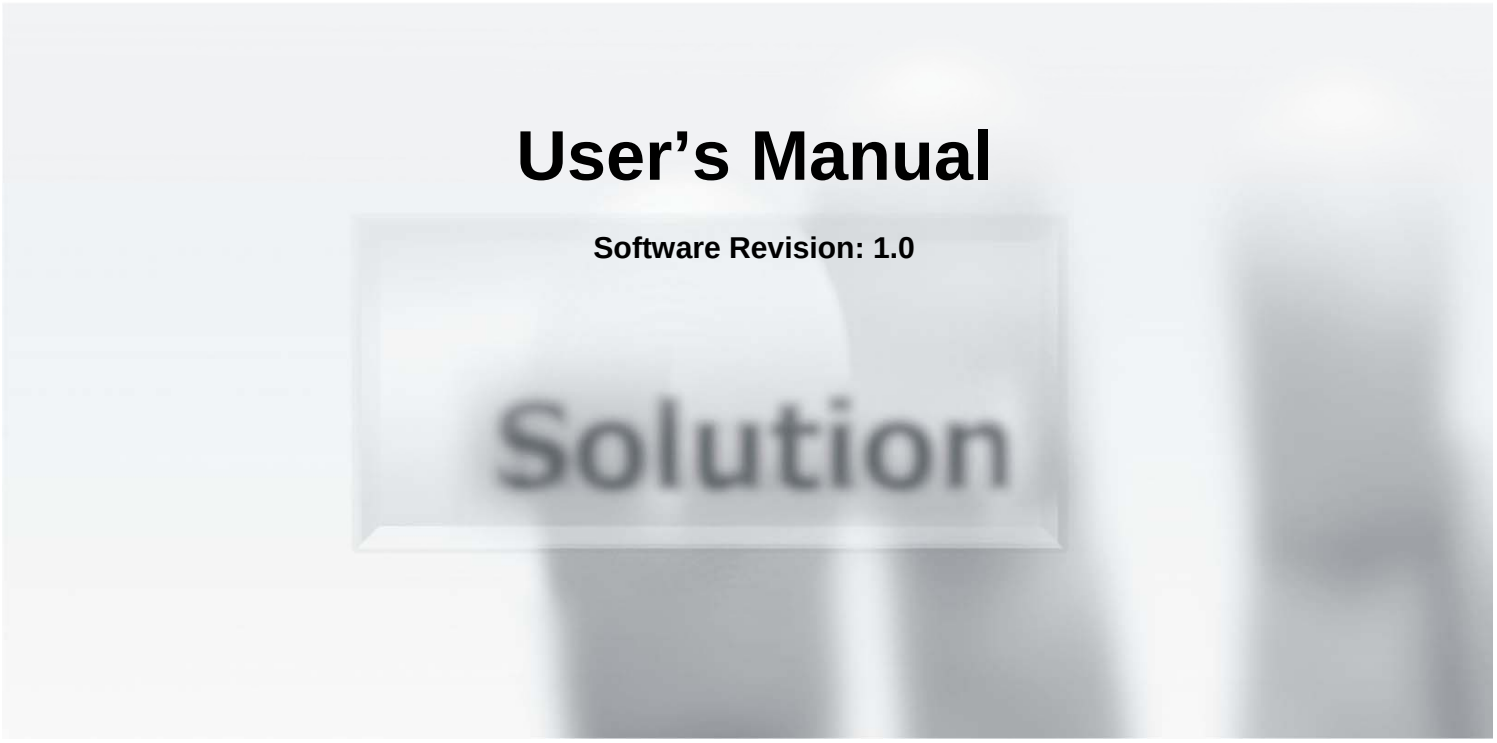
SANWatch®

Effortless RAID Management

Java-based GUI Manager for Infortrend RAID Subsystems

User's Manual

Software Revision: 1.0



Version 1.0 (May, 2007)

Contact Information

Asia Pacific
(International Headquarters)
Infortrend Technology, Inc.
8F, No. 102 Chung-Shan Rd., Sec. 3
Chung-Ho City, Taipei Hsien, Taiwan
Tel: +886-2-2226-0126
Fax: +886-2-2226-0020
sales.ap@infortrend.com
support.ap@infortrend.com
http://esupport.infortrend.com.tw
http://www.infortrend.com.tw

Americas
Infortrend Corporation
2200 Zanker Road, Unit D,
San Jose, CA. 95131
USA
Tel: +1-408-988-5088
Fax: +1-408-988-6288
sales.us@infortrend.com
http://esupport.infortrend.com
http://www.infortrend.com

China
Infortrend Technology, Limited
Room 1210, West Wing, Tower One, Junefield Plaza, No. 6 Xuanwumen Street, Xuanwu District, Beijing, China
Post code: 100052
Tel: +86-10-6310-6168
Fax: +86-10-6310-6188
sales.cn@infortrend.com
support.cn@infortrend.com
http://esupport.infortrend.com.tw
http://www.infortrend.com.cn

Europe (EMEA)
Infortrend Europe Limited
1 Cherrywood, Stag Oak Lane
Chineham Business Park
Basingstoke, Hampshire
RG24 8WF, UK
Tel: +44-1256-707-700
Fax: +44-1256-707-889
sales.eu@infortrend.com
support.eu@infortrend.com
http://esupport.infortrend-europe.com/
http://www.infortrend.com

Japan
Infortrend Japan, Inc.
6F, Okayasu Bldg.,
1-7-14 Shibaura Minato-ku,
Tokyo, 105-0023 Japan
Tel: +81-3-5730-6551
Fax: +81-3-5730-6552
sales.jp@infortrend.com
support.jp@infortrend.com
http://esupport.infortrend.com.tw
http://www.infortrend.co.jp

Copyright 2007

First Edition Published 2007

All rights reserved. This publication may not be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written consent of Infortrend Technology, Inc.

Disclaimer

Infortrend Technology makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Infortrend Technology reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation to notify any person of such revisions or changes. Product specifications are also subject to change without prior notice.

Trademarks

Infortrend, Infortrend logo, EonStor, RAIDWatch, and SANWatch are all registered trademarks of Infortrend Technology, Inc. Other names prefixed with "IFT" and "ES" are trademarks of Infortrend Technology, Inc.

Microsoft, Windows, Windows NT, Windows 2000, Windows XP, and Windows Server 2003, and Windows Storage Server 2003 are registered trademarks of Microsoft Corporation in the U.S. and other countries.

LINUX is a trademark of Linus Torvalds. RED HAT is a registered trademark of Red Hat, Inc.

Solaris and Java are trademarks of Sun Microsystems, Inc.

All other names, brands, products or services are trademarks or registered trademarks of their respective owners.

Table of Contents

CONTACT INFORMATION ..... **II**
COPYRIGHT 2007 ..... **III**
First Edition Published 2007 iii
Disclaimer iii
Trademarks iii
TABLE OF CONTENTS ..... **IV**
LIST OF TABLES ..... **X**
TABLE OF FIGURES ..... **X**

CHAPTER 1 INTRODUCTION

1.1 SANWATCH OVERVIEW **1-2**
1.1.1 Product Description 1-2
1.1.2 SANWatch Versions 1-2
1.1.3 Feature Summary 1-2
1.2 FEATURED HIGHLIGHTS **1-3**
1.2.1 Graphical User Interface (GUI) 1-3
1.2.2 Enclosure View 1-4
1.2.3 Powerful Event Notification 1-5
1.2.4 Java-based Remote Management 1-5
Mode One: Centralized Management 1-6
Mode Two: Stand-alone (on Host) 1-7
Mode Three: Stand-alone (on Subsystems) 1-7
Access Requirements 1-8
1.2.5 Multi-Language Support 1-11
1.2.6 Password Protection 1-11
1.3 CONCEPTUAL FOUNDATION **1-11**
1.3.1 Centralized Management (Agent-based) Installation 1-12
1.3.2 Stand-alone (on Host) Installation 1-13
1.3.3 Stand-alone (on Subsystem) Installation 1-13

CHAPTER 2 SANWATCH CONSIDERATIONS

2.1 BACKGROUND INFORMATION **2-2**
2.2 DEFINITION OF TERMS **2-2**
2.3 OPERATING WITH SPARE DRIVES **2-3**
2.4 OPERATING WITHOUT SPARE DRIVES **2-3**
2.5 BEFORE YOU START **2-4**

CHAPTER 3 INSTALLATION

3.1 SYSTEM REQUIREMENTS **3-2**
3.1.1 Servers Running SANWatch 3-2
3.1.2 Local Client Running SANWatch Manager 3-3
3.2 RAID CHART **3-4**
3.3 PLATFORM REQUIREMENTS **3-5**
3.4 SOFTWARE SETUP **3-5**
3.4.1 Before You Start 3-6
3.4.2 Installing SANWatch on a Windows Platform 3-6
3.4.3 Installing SANWatch on a Linux Platform 3-7
3.4.4 Installing SANWatch on a Solaris Platform 3-8
3.4.5 Installing SANWatch on a Mac OS Running Safari Browser 3-10
3.4.6 Installing SANWatch Main Program (for all platforms) 3-13
3.4.7 Installing Software Components 3-16
3.4.8 Stand-alone (on Host or Subsystem) Installation 3-19
3.5 USING SNAPSHOT (DATA SERVICE) **3-21**
3.6 PROGRAM UPDATES **3-22**
3.6 IN-BAND SCSI **3-23**
3.6.1 Overview 3-23

3.6.2 Related Configuration on Controller/Subsystem 3-23

CHAPTER 4 CONFIGURATION CLIENT OPTIONS

4.1 THE CONFIGURATION CLIENT UTILITY 4-2
4.1.1 Start the Configuration Client Program 4-2
4.1.2 Setting Up a Root Agent 4-4
4.2 CONFIGURATION CLIENT USER INTERFACE 4-7
4.2.1 Command Menu 4-7
4.2.2 Tool Bar Buttons 4-8
4.2.3 Connection View Window 4-8
4.2.4 Module Configuration Window 4-9
4.3 ROOT AGENT CONFIGURATION 4-10
4.3.1 Root Agent Settings 4-10
4.3.2 Adding RAID Agents IPs (Associating Root Agent with Multiple RAID Arrays) 4-11
4.3.3 Root Agent Log Settings 4-12
4.3.4 Create Plug-ins with Event Notification 4-13
Step 1. Before you begin 4-13
Step 2. The Configuration Process 4-13
4.4 EVENT NOTIFICATION SETTINGS 4-15
4.4.1 Configuration Client Notification Methods 4-15
4.4.2 Event Severity Levels 4-15
4.4.3 Enabling Notification Functions 4-16
4.4.4 SNMP Traps Settings 4-17
Receiver Side 4-17
Sender Side 4-19
4.4.5 Email Settings 4-19
Receiver Side 4-19
Sender Side 4-20
4.4.6 LAN Broadcast Settings 4-21
Receiver Side 4-21
Sender Side 4-23
4.4.7 Fax Settings 4-23
Receiver Side 4-23
Sender Side 4-25
4.4.8 MSN Settings 4-26
Receiver Side 4-26
Sender Side 4-27
4.4.9 SMS Settings 4-28
Receiver Side 4-28
Sender Side 4-29
4.5 AUTO DISCOVERY 4-31
4.6 EVENT SEVERITY LEVELS 4-33
4.6.1 Level 1 Severity Events (Examples) 4-33
4.6.2 Level 2 Severity Events (Examples) 4-34
4.6.3 Level 3 Severity Events (example) 4-34
4.7 EVENT LOG DISPLAY 4-35

CHAPTER 5 SANWATCH ICONS

5.1 NAVIGATION TREE ICONS 5-1
5.2 ARRAY INFORMATION ICONS 5-3
Enclosure View 5-3
Tasks Under Process 5-4
Logical Drive Information 5-4
Logical Volume Information 5-4
Fibre Channel Status 5-5
System Information 5-5
5.3 MAINTENANCE ICONS 5-5
Maintenance 5-5
5.4 CONFIGURATION ICONS 5-6

Create Logical Drives 5-6
Existing Logical Drives 5-6
Create Logical Volume 5-6
Existing Logical Volumes 5-6
Host Channel 5-6
Host LUN Mapping 5-7
Configuration Parameters 5-7
5.5 EVENT LOG ICONS 5-7
Event Messages 5-7

CHAPTER 6 BASIC OPERATIONS

6.1 STARTING SANWATCH AGENTS 6-3
6.2 STARTING SANWATCH MANAGER 6-4
6.2.1 Locally or via LAN under Windows 2000/ 2003 Environments 6-4
6.2.2 Locally or via LAN under Linux Environments 6-5
6.2.3 Locally or via LAN under Solaris Environments 6-5
6.2.4 For Remote Management via Web Browser (Any Supported OSes) 6-5
6.3 START USING SANWATCH MANAGER 6-6
6.3.1 Purchasing the License Key 6-7
6.3.2 Connecting to a RAID Subsystem 6-9
6.3.3 Using the Agent List Window 6-11
6.3.4 Disconnecting and Refreshing a Connection 6-13
6.4 SECURITY: AUTHORIZED ACCESS LEVELS 6-13
6.5 LOOK AND FEEL 6-14
6.5.1 Look and Feel Overview 6-14
6.5.2 Screen Elements 6-15
6.5.3 Command Menus 6-15
6.5.4 Outer Shell Commands 6-16
6.5.5 Management Window Commands 6-17
6.6 THE INFORMATION CATEGORY 6-18
6.6.1 Enclosure View Window 6-18
6.6.2 Tasks Under Process Window 6-19
6.6.3 Logical Drive Information Window 6-19
6.6.4 Logical Volume Information Window 6-20
6.6.5 Fibre Channel Status Window 6-21
6.6.6 System Information Window 6-21
6.6.7 Statistics Window 6-22
Cache Dirty (%) 6-22
Disk Read/Write Performance (MB/s) 6-22
6.7 THE MAINTENANCE CATEGORY 6-22
6.7.1 Logical Drive Maintenance Window 6-23
6.7.2 Physical Drives Maintenance Window 6-25
6.7.3 Task Schedules Maintenance Window 6-27
6.8 THE CONFIGURATION CATEGORY 6-28
6.8.1 Quick Installation 6-28
6.8.2 Create Logical Drive Window 6-28
6.8.3 Existing Logical Drives Window 6-29
6.8.4 Create Logical Volume Window 6-30
6.8.5 Existing Logical Volumes Window 6-30
6.8.6 Channel Window 6-31
6.8.7 Host LUN Mapping Window 6-32
6.8.8 Configuration Parameters Window 6-33
6.9 ARRANGING WINDOWS 6-33
6.10 MULTI-ARRAY MANAGEMENT 6-34

CHAPTER 7 CONFIGURATION PARAMETERS

7.1 ACCESSING THE CONFIGURATION PARAMETERS OPTIONS 7-2
7.2 COMMUNICATIONS 7-3
7.3 CONTROLLER 7-4

7.4 SYSTEM 7-6
7.5 PASSWORD 7-8
7.6 THRESHOLD 7-9
7.7 REDUNDANT CONTROLLER SETTINGS 7-10
7.8 EVENT TRIGGERED OPERATIONS 7-13
7.9 HOST-SIDE, DRIVE-SIDE, AND DISK ARRAY PARAMETERS 7-13

CHAPTER 8 CHANNEL CONFIGURATION

8.1 CHANNEL CONFIGURATION WINDOW 8-2
8.2 USER-CONFIGURABLE CHANNEL PARAMETERS 8-3
Channel Parameters: EonStor Series 8-3
Channel Parameters: EonStor 1U Controller Head Series 8-4
8.2.1. Channel Mode 8-4
8.2.2. Termination 8-5
8.2.3. Default Transfer Clock (in MHz) 8-5
8.2.4. ID Pool / AID / BID 8-6
8.3 SETTING THE CONFIGURATIONS FOR A CHANNEL 8-7

CHAPTER 9 DRIVE MANAGEMENT

9.1. LOCATING DRIVES 9-3
9.2. LOGICAL DRIVE MANAGEMENT 9-3
9.2.1 Accessing the Create Logical Drive Window 9-4
9.2.2 Creating Logical Drives 9-5
9.2.2.1. Logical Drive Creation Process 9-5
9.2.2.2. Selecting Drives 9-5
9.2.2.3. Setting RAID Parameters 9-6
Drive Size 9-6
Selecting Stripe Size 9-6
Initialization Options 9-6
Select RAID Level 9-6
Write Policy 9-6
9.2.2.4. Click OK to Create an LD 9-7
9.2.3 Accessing the Existing Logical Drive Window 9-7
9.2.3.1. Modifying LD Configurations 9-9
9.2.3.2. Expanding LD by Adding Disks 9-9
9.2.3.3. Accessing the Expand Command page 9-10
Available Expansion Size (MB) 9-10
Set Expansion Size 9-10
Execute Expand 9-11
9.2.3.4. Click Expand to Initiate LD Expansion 9-11
9.2.3.5. Accessing the Migrate LD Command page 9-11
Select a RAID Level 9-12
Select a Stripe Size 9-12
Set a Drive Size 9-13
9.2.3.6. Migration Process 9-13
9.2.4 Dynamic Logical Drive Expansion 9-13
9.2.4.1. What Is It and How Does It Work? 9-13
9.2.4.2. Two Expansion Modes 9-13
Mode 1: Add Drive 9-13
Mode 2: Copy & Replace 9-14
9.2.5 Adding Spare Drives 9-16
9.2.5.1. Accessing the Spare Drive Management Screen 9-17
9.2.6 Rebuilding Logical Drives 9-18
9.2.7 Deleting an LD 9-18
9.3. LOGICAL VOLUME MANAGEMENT 9-20
9.3.1 Accessing the Create Logical Volume Window 9-20
9.3.2 Creating Logical Volumes 9-21
9.3.2.1. LV Creation 9-21
9.3.2.2. Selecting LDs 9-21
9.3.2.3. Setting Logical Volume Parameters 9-22
Logical Volume Assignment 9-22
Select Write Policy 9-22

9.3.2.4. Click OK to Create a Logical Volume 9-22
9.3.3 Accessing the Existing Logical Volumes Window 9-23
9.3.3.1. Modifying Logical Volume Configurations 9-24
9.3.3.2. Expanding a Logical Volume 9-24
9.3.3.3. Accessing the Expand Logical Volume Page 9-25
9.3.4 Deleting a Logical Volume 9-26
9.4. PARTITIONING A LOGICAL CONFIGURATION 9-27
9.4.1 Overview 9-27
9.4.2 Partitioning a Logical Drive 9-27
9.4.3 Partitioning a Logical Volume 9-29
9.5. PHYSICAL DRIVE MAINTENANCE 9-31
9.5.1 Read/Write Test 9-31

CHAPTER 10 LUN MAPPING

10.1. ACCESSING THE LUN MAP TABLE 10-2
10.2. LUN MAPPING 10-4
10.2.1. Mapping a Complete Logical Drive or Logical Volume 10-4
10.2.2. Map a Logical Drive or Volume Partition to a Host LUN 10-5
10.2.3. Deleting a Host LUN Mapping 10-5
10.2.4. LUN Mapping Access Control over iSCSI Initiator Settings 10-6

CHAPTER 11 SYSTEM MONITORING AND MANAGEMENT

11.1 RAID INFORMATION 11-2
The Information Category 11-2
Date and Time 11-3
11.2 ENCLOSURE VIEW 11-4
Task Under Process 11-4
Event Log List/Configuration List Window 11-5
11.3 LOGICAL DRIVE INFORMATION 11-8
Accessing Logical Drive Information 11-9
11.4 LOGICAL VOLUME INFORMATION 11-10
Accessing Logical Volume Information 11-10
11.5 FIBRE CHANNEL STATUS 11-11
11.6 SYSTEM INFORMATION 11-11

CHAPTER 12 ENCLOSURE DISPLAY

12.1 ABOUT THE ENCLOSURE VIEW WINDOW 12-2
12.2 ACCESSING THE ENCLOSURE VIEW 12-2
12.2.1 Connecting to the RAID Agent 12-2
12.2.2 Opening the Enclosure View Window 12-2
12.2.3 Component Information 12-3
12.3 LED REPRESENTATIONS 12-4
12.3.1 Service LED (on Models that Come with an LED panel) 12-4
12.4 ENCLOSURE VIEW MESSAGES 12-5
12.5 INFORMATION SUMMARY 12-6

CHAPTER 13 NPC UTILITY INSTALLATION

13.1. THE NPC UTILITY 13-2
13.1.1 Introduction 13-2
13.1.2 To Access the Utility 13-2
13.2. CONFIGURING THE UTILITY OPTIONS 13-3
13.2.1 SSL 13-3
13.2.2 Email Notification 13-3
13.2.3 SNMP Traps 13-5
13.2.4 Broadcast Notification 13-6

CHAPTER 14 CENTRAL MANAGEMENT UTILITY

14.1. CENTRALIZED MANAGEMENT INTRODUCTION 14-2

14.2. SETTING UP THE UTILITY 14-2
14.3. CENTRAL MANAGEMENT CONNECTION 14-4
14.4. MAINTENANCE & CONFIGURATION 14-4
14.4.1 Icon Labels 14-4
14.4.2 System Events 14-5

CHAPTER 15 DATA SERVICE: SNAPSHOT

15.1 SNAPSHOT BASICS 15-1
15.2 CONFIGURATION PROCESS 15-4
Using the SANWatch: License Login 15-4
GUI Structure 15-8
Snapshot General Configuration Process 15-14
Configuration Steps: 15-16
Other Commands: 15-25
15.3 SNAPSHOT PURGE POLICY (SPACE MANAGEMENT) 15-28
15.4 SNAPSHOT SCHEDULER & PRUNE POLICY CONFIGURATION 15-33

APPENDICES

APPENDIX A COMMAND SUMMARY A-2
A.1. Menu Commands A-2
A.2. RAID Watch Program Commands A-2
SANWatch System Menu Commands (Outer-Shell Window) A-2
SANWatch Language menu Commands (Outer-Shell Window) A-2
SANWatch Window Menu Commands (Outer-Shell Window) A-3
SANWatch Help Menu Commands (Outer-Shell Window) A-3
SANWatch System Menu Commands (Management Window) A-3
SANWatch Action Menu Commands (Management Window) A-4
A.3. Configuration Client Utility Commands A-4
File Menu Commands A-4
Language Selection Commands A-4
Help Menu Commands A-4
Tool Bar Commands A-5
Root Agent Right-click Menu Commands A-5
APPENDIX B GLOSSARY A-7
APPENDIX C RAID LEVELS A-13
C.1. RAID Description A-13
C.2. Non-RAID Storage A-13
C.3. RAID 0 ..... A-14
C.4. RAID 1 ..... A-15
C.5. RAID 1(0+1) A-15
C.6. RAID 3 ..... A-16
C.7. RAID 5 ..... A-17
C.8. RAID 6 ..... A-18
C.9. RAID 10, 30, 50 and 60 ..... A-18
APPENDIX D ADDITIONAL REFERENCES A-19
D.1. Java Runtime Environment A-19
D.2. SANWatch Update Downloads & Upgrading A-19
D.3. Uninstalling SANWatch A-19

USER'S MANUAL OVERVIEW XII
USER'S MANUAL STRUCTURE AND CHAPTER OVERVIEWS XII
Part 1: Getting Started With SANWatch xii
Part 2: Using SANWatch for System Management xiii
Part 3: System Monitoring xiii
Part 4: Data Service xiv
Appendices xiv
USAGE CONVENTIONS XV

SOFTWARE AND FIRMWARE UPDATES XVI
REVISION HISTORY XVI

List of Tables

Table 1-2: Software Modules with Different SANWatch Installations 9
Table 1-2: Software Modules: SANWatch Console over Browser-invoked Java Applet 10
Table 1-3: Software Modules: Management Only 10
Table 1-5: SANWatch Module Requirements 13
Table 3-1: RAID Charting Table 4
Table 4-1: Levels of Notification Severity 16
Table 7-1: Peripheral Device Type Parameters 17
Table 7-2: Peripheral Device Type Settings 17
Table 7-3: Cylinder/Head/Sector Mapping under Sun Solaris 18
Table 7-4: Cylinder/Head/Sector Mapping under Sun Solaris 18
Table 8-1: Dual-Redundant Controller Channel Modes 4
Table 8-2: Dual-Single Controller Channel Modes 4
Table 8-3: SCSI Channels Clock Speeds 5
Table 10-1: iSCSI Initiator CHAP Configuration Entries 8
Table 11-1: Array Information Icons 3
Table 11-2: Severity Level Icons 6
Table 11-3: Device Icon 12

List of Figures

Figure 1-3: Centralized, Tiered Management 6
Figure 1-2: Mode Two, Stand-alone for In-band Management 7
Figure 1-3: Mode Three, Applet Mode Management 8
Figure 1-4: Typical SANWatch Connection – Heterogeneous 9
Figure 1-5: Typical SANWatch Connection – Applet Mode 10
Figure 1-6: Typical SANWatch Access – the Applet Mode 10
Figure 4-1: Configuration Client Shortcut on Windows Startup Menu 3
Figure 4-2: Connection: The Right-click Menus 9
Figure 4-3: Enabling a Notification Method by the Switch Button 17
Figure 4-4: Adding Email Notification 20
Figure 4-5: The Root Agent List 33
Figure 6-1: SANWatch Shortcuts on Windows Startup Menu 4
Figure 6-2: SANWatch Shortcut on Windows Desktop 4
Figure 6-3: Ending a Management Session with a Connected Array 13
Figure 6-4: GUI Screen Elements 15
Figure 6-5: Command Menu Bar 16
Figure 6-6: Outer Shell Commands 16
Figure 6-7: Management Window Commands 17
Figure 6-8: Accessing Information Commands 18
Figure 6-9: Enclosure View Window 19
Figure 6-10: Task Status Window 19
Figure 6-11: Logical Drive information 20
Figure 6-12: Logical Volume Information 20
Figure 6-13: Fibre Channel Status Window 21
Figure 6-14: System Information Window 21
Figure 6-15: Performance Statistics Window 22
Figure 6-16: Accessing Maintenance Commands 23
Figure 6-17: Maintenance - Logical Drives 23
Figure 6-18: Maintenance - Physical Drives 25
Figure 6-19: Task Schedules Window 27
Figure 6-20: Accessing Configuration Commands 28
Figure 6-21: Selecting Members for a New Logical Drive 29

Figure 6-22: Existing Logical Drives Window 30
Figure 6-23: Channel Window 31
Figure 6-24: Host Channel ID Settings 32
Figure 6-25: Host LUN Mapping Right-click Menu 32
Figure 6-26: The "Outer Shell" System View Window 33
Figure 6-27: Opening Device for Multi-Array Management 34
Figure 7-2: The Host-side Parameters Page for iSCSI Models 19
Figure 9-1: Access to the Create Logical Drive Window 4
Figure 9-2: Accessing the Existing Logical Drives Window 8
Figure 9-3: RAID Expansion Mode 1 14
Figure 9-4: RAID Expansion Mode 2 (1/3) 14
Figure 9-5: RAID Expansion Mode 2 (2/3) 15
Figure 9-6: RAID Expansion Mode 2 (3/3) 15
Figure 9-7: Accessing the Create Logical Volume Window 20
Figure 9-8: Accessing Existing Logical Volume Window 23
Figure 12-1: EonRAID 2510FS Enclosure View 2
Figure 12-2: EonStor F16F Series Enclosure View 2
Figure 12-3: Enclosure Tabbed Panel and Component LED Display 4
Figure 12-4: Service LEDs 5
Figure 12-5: Component Information Message Tags 5
Figure 12-6: Information Summary 6
Figure 14-1: Not Connected 4
Figure 14-2: Data Query 4
Figure 14-3: Connected 4
Figure 14-4: Connecting 4
Figure 15-1: Snapshots through a Time Line 1
Figure 15-2: Snapshot Relevant Directory Architecture 3
Figure 15-3: License Key Application Procedure 4
Figure 15-4: The Intermediate RAID Agents on a Direct-attached Server 9
Figure 15-5: Snapshot General Configuration Process 14
Figure 15-6: Array Space Allocation in Snapshot Application 16
Figure 15-7: Exemplary RAID and Snapshot Configuration Drawing 18
Figure 15-8: Snapshot Image Mapped to Host ID/LUN (Data Retrieval) 24
Figure 15-9: Snapshot Purge Policy 28
Figure 15-10: Snapshot Prune Policy 29
Figure 15-11: Purge Policy on One of the Snapshot Sets 30
Figure C-1: Non-RAID Storage 14
Figure C-2: RAID0 Storage 14
Figure C-3: RAID1 Storage 15
Figure C-4: RAID 1(0+1) Storage 16
Figure C-5: RAID 3 Storage 17
Figure C-6: RAID 5 Storage 17
Figure C-7: RAID 6 Storage 18
Figure D-1: SANWatch Uninstallation Program 19

User's Manual Overview

Congratulations on your decision to use Infortrend's SANWatch management software program. This management program allows you to control and monitor disk array subsystems from a local host, a remote station connected through a local area network (LAN), In-band host links, or the Internet.

This manual discusses how to install and use SANWatch to manage disk array systems incorporating Infortrend's Fibre-to-Fibre, Fibre-to-SATA/SAS, SCSI-to-SATA, SAS-to-SAS/SATA, iSCSI-to-SATA, and SCSI-to-SCSI subsystems, or the EonRAID 2510FS series controllers. Please note that SANWatch does not support drive enclosures manufactured by other vendors.

In addition to SANWatch, you can also use the serial COM port or LCD keypad panel to manage the EonStor subsystems or systems that incorporate the EonRAID disk array controllers. For more information about these programs, see the documentation that came with your hardware.

User's Manual Structure and Chapter Overviews

Chapters in this SANWatch User's Manual are included in four (4) separate parts and Appendices.

Part 1: Getting Started With SANWatch

Chapter 1: Introduction

Provides information about SANWatch, including a product description, features summary and highlights. The basic concept of SANWatch is defined in an individual section.

Chapter 2: SANWatch Considerations

Provides some background information on RAID and defines some terms that will be used throughout the rest of the manual. Discusses the use of spare drives and how to replace a drive if no spares were available. Finally, provides a short discussion on SANWatch preliminaries.

Chapter 3: Installation

Discusses how to install SANWatch in your systems. Discussions include system requirements, setting up hardware, software installation, and how to update your software by downloading updates from Infortrend's websites.

Chapter 4: Configuration Client Options

Describes how to configure the SANWatch's Configuration Client utility and event notification for faxes, e-mail, broadcast, and so on. Other functionalities of the utility

are also described in full. Information about the supported notification levels is also provided to aid in explaining these functions.

Chapter 5: SANWatch Icons

Describes the icons used in SANWatch GUI.

Chapter 6: Basic Operations

Discusses basic operations at system startup. These include starting SANWatch, connecting and disconnecting from a disk array system, setting up system security, displaying controls, working with various disk array windows, and exiting the program.

Part 2: Using SANWatch for System Management

Chapter 7: Configuration Parameters

Discusses how to access the controller/subsystem configuration options and the different RAID configuration options that are available. A detailed description of how to set these options is given as well as brief explanations of the different parameters.

Chapter 8: Channel Configuration

Discusses how to access the I/O channel-related configuration options and describes in detail the user-configurable channel options. Instructions on setting the configuration of a channel and how to configure host channel IDs are also discussed.

Chapter 9: Drive Management

This chapter describes the creation, expansion and deletion of both logical drives (LD) and logical volumes (LV). Different LD and LV options are explained and steps to setting the different options are described in detail. A discussion on partitioning LDs and LVs is also found in this chapter.

Chapter 10: LUN Mapping

Discusses how to map complete LDs or separate partitions within LDs and LVs to different LUNs. Detailed description of the mapping procedure is given. A discussion on how to delete LUN mappings and a description of the LUN Mapping Table are provided. All the associated options are also described.

Part 3: System Monitoring

Chapter 11: System Monitoring & Management

Discusses how to obtain the current status of devices monitored through SAF-TE, I^2C, and S.E.S. interfaces and get updates on the status of storage system components. Descriptions on how to access these different monitoring devices are given and the type of information that is offered by these devices is shown.

Chapter 12: Enclosure Display

The Enclosure View customization is discussed fully in this chapter. Detailed instructions on how to access and use the Enclosure View are given. Examples of status messages are shown and explanations of the status messages are provided.

Chapter 13: NPC Utility

An independent NPC configuration utility is added for use with SANWatch installation without the Configuration Client functionality. Although not as powerful as the Configuration Client, NPC provides basic event notifications over email, LAN broadcast, and SNMP traps.

Chapter 14: Central Management Utility

The Central Management utility provides an online, one-to-many monitoring capability of Infortrend RAID subsystems over the network, enhancing ease of use for managing a storage network.

Part 4: Data Service

Chapter 15: Data Service: Snapshot Operation

Discusses how to start, configure point-in-time snapshots, and maintain a balanced distribution of capacity between ordinary RAID volumes and snapshot volumes. Details about the automated snapshot scheduler utility can also be found.

Appendices

Appendix A: Command Summary

Summarizes the available commands and command buttons within SANWatch (RAID management part) and the Configuration Client utility.

Appendix B: Glossary

Provides information on definitions of key technology terms used in this manual.

Appendix C: RAID Levels

Provides information about the various RAID levels.

Appendix D: Additional References

Provides information about Java Runtime environment, software download, and uninstallation.

Usage Conventions

Throughout this document, the following terminology usage rules apply:

- "Controller" always refers to Infotrend RAID array controllers.
- "Subsystem" refers to Infortrend EonStor 8-, 12-, 16-bay, or 24-bay RAID array subsystems.
- "SANWatch" refers to the entire program and all of its modules.
- "SANWatch Manager" refers only to the management interface, not to any other parts of the software.
- "Root Agent" is an independent agent of the software, which permits one management station to monitor and report the operating status of multiple RAID systems. The Root Agent acquires information from and sends configuration commands to one or multiple RAID arrays.
- "RAID Agent" is the part of the software, which allows the RAID controller/subsystem to talk to the SANWatch Manager or Root Agent. A RAID Agent communicates with the RAID array via an Ethernet link, SCSI bus, iSCSI or Fibre channels (using the In-band protocols). RAID Agents are the intermediaries between RAID systems and the SANWatch program.
- "Configuration Client" refers to the software utility that allows an administrator to be notified of system events at any of the RAID systems being managed. The Configuration Client also enables centralized management of multiple arrays using a single workstation.

  Important information that users should be aware of is indicated using the following icons:

NOTE:

These messages inform the reader of essential but non-critical information. These messages should be read carefully as any directions or instructions contained therein can help you avoid making mistakes.

CAUTION!

Cautionary messages should also be heeded to help you reduce the chance of losing data or damaging the system.

IMPORTANT!

The Important messages contain information that might otherwise be overlooked or configuration details that can cause negative results.

WARNING!

Warnings appear where overlooked details may cause damage to the equipment or result in personal injury. Warnings should be taken seriously.

Software and Firmware Updates

Please contact your system vendor or visit Infortrend's esupport or VIProom websites for the latest software or firmware updates.

Problems that occur during the updating process may cause irrecoverable errors and system down time. Always consult technical personnel before proceeding with any firmware upgrade.

NOTE:

Firmware version installed on your system should provide the complete functionalities listed in the specification sheet/user's manual. We provide special revisions for various application purposes. Therefore, DO NOT upgrade your firmware unless you fully understand what a firmware revision will do.

Revision History

May 30, 2007

Initial release.

Chapter 1

Introduction

This chapter provides information about the SANWatch management program. The following topics are discussed in this chapter:

- **SANWatch Overview – Section 1.1, page 1-1**
  - **1.1.1 Product Description**
  - **1.1.2 SANWatch Versions**
- **Featured Highlights – Section 1.2, page 1-3**
  - **1.2.1 Graphical User Interface**
  - **1.2.2 Enclosure View**
  - **1.2.3 Powerful Event Notification**
  - **1.2.4 Java-based Remote Management**
- **Conceptual Foundation – Section 1.3, page 1-11**
  - **1.3.1 Centralized Management (Agent-based) Installation**
  - **1.3.2 Stand-alone (on Host) Installation**
  - **1.3.3 Stand-alone (on Subsystem) Installation**

1.1 SANWatch Overview

1.1.1 Product Description

Infortrend's innovated RAID manager, SANWatch, is a Java-based program specifically designed for use in managing Infortrend's RAID subsystems.

SANWatch provides a user-friendly interface that graphically represents disk array elements and simplifies the normally complicated process of array configuration. SANWatch also provides real-time reporting on the status of the entire array, thus making the task of monitoring disk arrays virtually effortless.

SANWatch complements the on-board console interface found on Infortrend's RAID controllers and a line of host-based, text mode RAID Managers that provide the same functionality, but with greater ease of use. The following sections describe SANWatch's outstanding features and introduce its conceptual framework.

1.1.2 SANWatch Versions

SANWatch is available in the **Express** and the **Professional** versions. The differences between them are about the snapshot functions. Following is a comparison chart of the two versions:

Specifications		Express	Professional
Capacity	No. of source volumes	4	Per system LD limitations
	Snapshots per source volume	8	128
	Max. no. of snapshots per system	32	Up to 1024 (depends on cache size and storage capacity
Online Snapshot Image Mapping		4	128
Snapshot Scheduler & Automated Prune		N/A	Yes
Space Threshold Setting & Automated Prune		N/A	Yes
Ready-only Access		Yes	Yes
OS Flush Agent support		Ye	Server2003

Table 1-1: Comparison between the Express and Professional Versions

A 30 days trial is provided with the software and you must purchase the software to continue using either the Express or the Professional version. Please refer to Chapter 3 for License Login details.

1.1.3 Feature Summary

The list below summarizes SANWatch features:

- Supports **Data Service**: point-in-time snapshot backup.
- Supports RAID level 6, which sustains the highest fault tolerance.

- RAID level migration on a per logical drive basis.
- Each logical drive can be managed by both RAID controllers.
- 512K/1024K stripe size supported.
- User-friendly graphical interface displays multiple information windows for simultaneous access to multiple RAID subsystems.
- Standard TCP/IP connections to an Internet agent for full-featured, worldwide management over the network.
- Communicates with RAID subsystems over a LAN (out-of-band) and the Internet, and over the existing host busses (SCSI, iSCSI, SAS, or Fibre links) using the in-band command protocols.
- Severity levels and display sequences are configurable for event notification.
- Provides password protection to guard against unauthorized modification of disk array configuration; passwords are set for Maintenance (user) and Configuration (administrator) login access.
- A **Centralized Management** utility that provides easy access to numerous RAID subsystems in the network.
- A **Configuration Client** utility that provides event notification via Email, Fax, MSN Messenger, SMS Short Message, LAN Broadcast, and SNMP Traps
- Compatible with most popular computer working environments: Windows, Linux, and Solaris operating systems with the Java Run-time Environment.

1.2 Featured Highlights

1.2.1 Graphical User Interface (GUI)

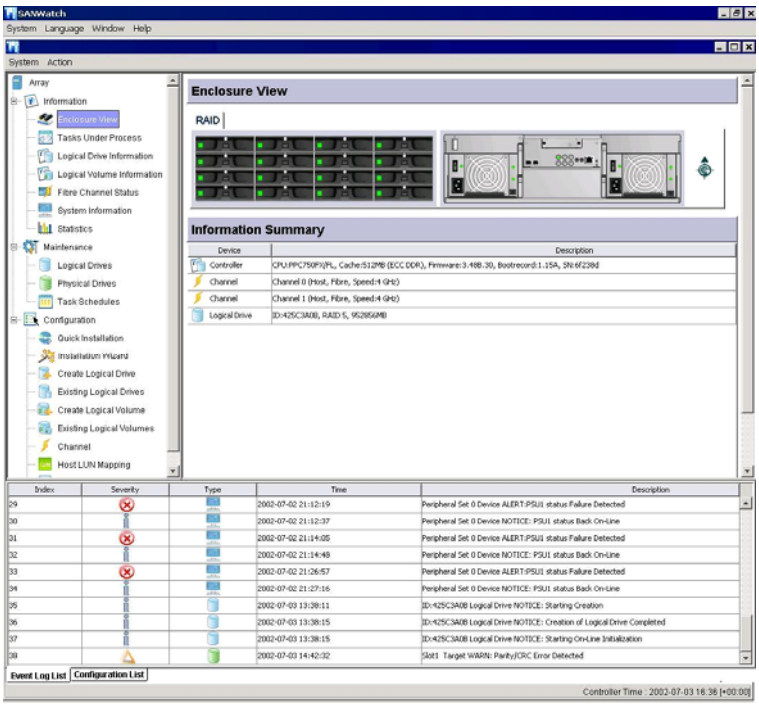
SANWatch manager is designed for ease-of-use. It uses symbolic icons to represent configuration levels, physical and logical drives, and logical volumes on the screen, and to identify the current configuration of a disk array system. Pull-down, right-click, and pop-up menus are used with all command options.

You need only point-and-click a mouse button to select an icon or command. The program also displays the current status of various disk drives or enclosure components by changing the color of their respective LED icons.

With an easy-to-use interface, complicated disk array operations such as logical drive and logical volume creation, drive partitioning, and LUN mapping to host channels/LUNs can be completed with just a few mouse clicks.

The Central Management utility, an entrance portal to SANWatch, provides convenient access to other management stations and to the RAID subsystems across storage networks. The utility also provides an instant event log, which can be exported to a text file.

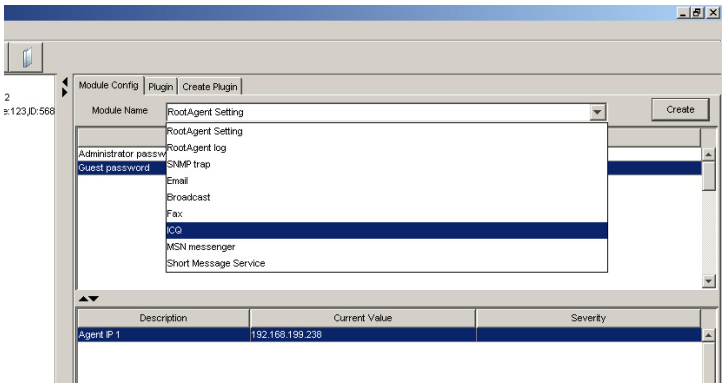
1.2.2 Enclosure View



The enclosure window shown above provides real-time reporting of the status of enclosure components, including components that can be accessed through the front or the rear side of an enclosure. When a drive fails, the system highlights the corresponding LED icon of the failed drive by changing its display color. When you remove a drive, its icon is removed from the enclosure window. This feature is particularly useful in cases when a drive fails, and you need to identify its exact location for subsequent replacement.

The enclosure window also appears in other configuration windows showing the logical relationship between the member drives of a logical configuration. Drives belonging to the same logical drive will be displayed in the same color. This allows you to easily identify members of different RAID configurations. The cascaded enclosures are access through a tabbed menu.

1.2.3 Powerful Event Notification

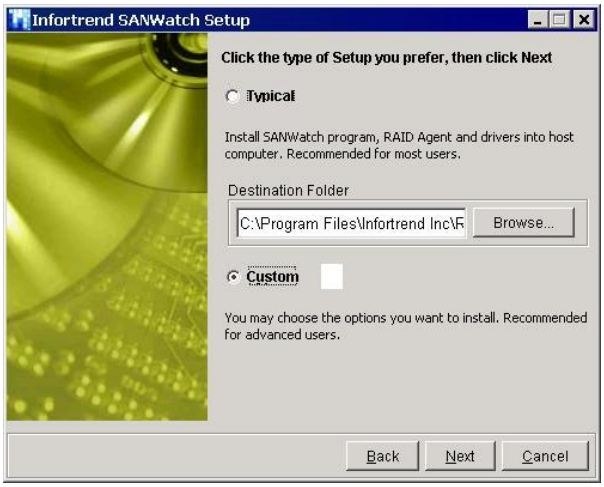


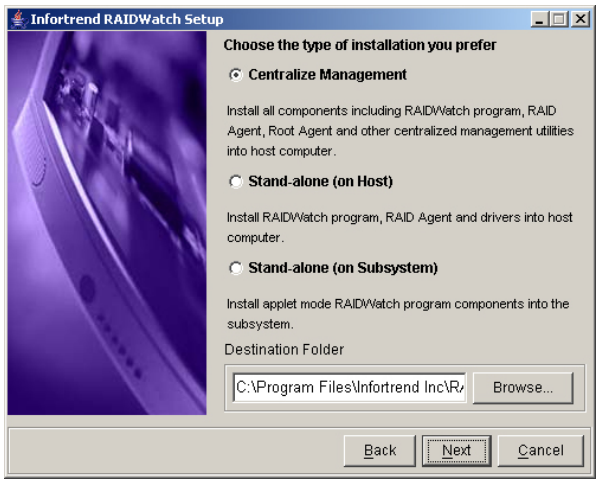
SANWatch can automatically notify system administrators of event occurrences and status changes. Event Notification is managed by a SANWatch's sub-module, **Configuration Client,** that is installed onto a management station and runs independently from the main manager program. Notifications can be sent via the Internet as email messages, via a local network as a broadcast message, SNMP traps, MSN messenger, SMS short message, or via fax/modem as fax messages without location constraints. To setup the event notification options, please refer to ***Chapter 4*** in this manual.

1.2.4 Java-based Remote Management

SANWatch supports local or remote management of Infortrend EonStor subsystems over a LAN or WAN using the TCP/IP protocol. SANWatch can be highly flexible in terms of its access routes to a RAID subsystem.

When the "**Custom**" installation mode is chosen during the installation process, three (3) installation schemes are available for you to select using the install shield program. Below sections are the explanations of the three Custom Mode options.


Infortrend SANWatch Setup
Click the type of Setup you prefer, then click Next
Typical
Install SANWatch program, RAID Agent and drivers into host computer. Recommended for most users.
Destination Folder
C:\Program Files\Infortrend Inc\R
Browse...
Custom
You may choose the options you want to install. Recommended for advanced users.
Back
Next
Cancel


Infortrend RAIDWatch Setup
Choose the type of installation you prefer
Centralize Management
Install all components including RAIDWatch program, RAID Agent, Root Agent and other centralized management utilities into host computer.
Stand-alone (on Host)
Install RAIDWatch program, RAID Agent and drivers into host computer.
Stand-alone (on Subsystem)
Install applet mode RAIDWatch program components into the subsystem.
Destination Folder
C:\Program Files\Infortrend Inc\R
Browse...
Back
Next
Cancel

NOTE:

The **Typical** mode installation equals the **Stand-alone (on Host)** mode among the Custom mode options.

- ## Mode One: Centralized Management

For centralized or one-to-many configurations using either the Ethernet or in-band host connection to the RAID subsystems. The **root agent** and utility sub-modules, including the **Configuration Client** and **Central Management**, are included. Necessary RAID agents are installed onto the management computer.

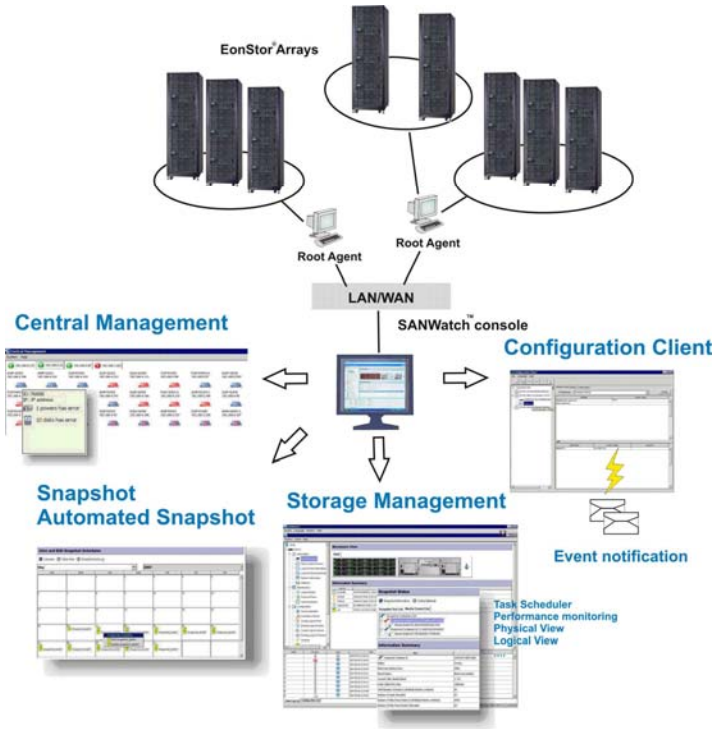


Figure 1-1: Centralized, Tiered Management

- ## Mode Two: Stand-alone (on Host)

Mode Two applies to configurations that depend on the existing SCSI, iSCSI, SAS, or Fibre host links for SANWatch-to-RAID communications using the in-band protocols. Servers in DAS (Direct Attached Storage) environments, SCSI host models for example, require RAID agents as the intermediate module for passing SANWatch commands and communicating with RAID system firmware. RAID agents are installed onto the servers that are directly attached to a RAID subsystem.

The **Mode Two** installation is especially necessary in **Snapshot** applications where the specialized **RAID Agents** also function as flush agents. SANWatch needs to be installed using Mode Two on a direct-attached server.

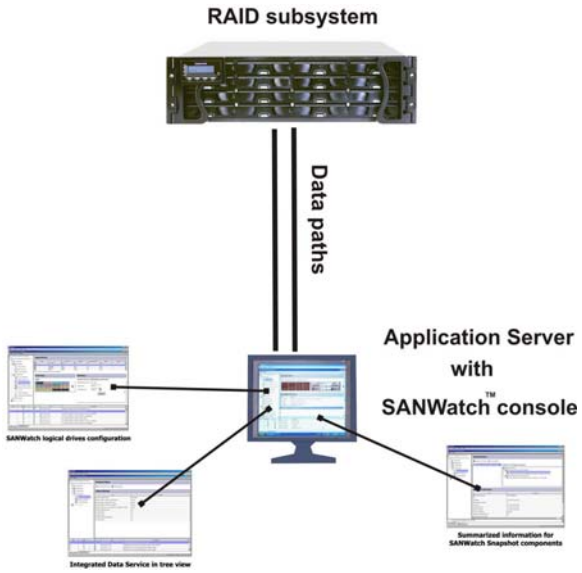


Figure 1-2: Mode Two, Stand-alone for In-band Management

- ## Mode Three: Stand-alone (on Subsystems)

For remote and server-transparent management using an Ethernet connection to EonStor subsystems or EonRAID controllers. The manager program is installed onto the RAID subsystem itself. The RAID subsystem then uses a segregated disk space, called the “reserved space,” to store the program files. The array is accessed by invoking a Java Applet on a web browser that runs anywhere in the network.

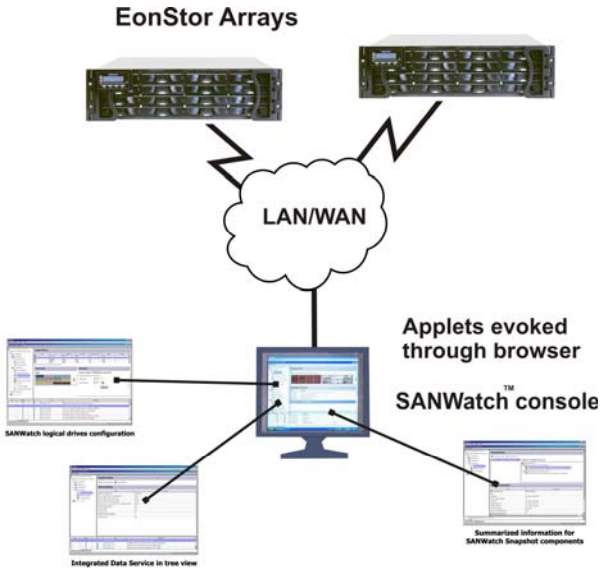


Figure 1-3: Mode Three, Applet Mode Management

NOTE:

RAID agents are embedded in the RAID subsystem firmware. A management station running the Mode 1 components can manage arrays accessed through Mode 2 or Mode 3 components. This way, multiple and/or distant arrays can be managed by a single management station.

- ## Access Requirements

Three (3) installation schemes for different access requirements are discussed below.

NOTE:

The discussions below do not include all possibilities. SANWatch supports various configurations and the combinations of machines running components installed in any of the three different modes.

1. **A RAID Server Chosen as the Centralized Management Station**: Applied in heterogeneous environments where multiple arrays are serving different hosts/applications and are scattered in distant locations. Access management over the network is achieved through data exchanges between a local or remote SANWatch Manager station (can be a RAID server or not) and RAID agents that are installed on the RAID servers or RAID subsystems themselves. The management center and the SANWatch station can be two different machines.

   A Root agent is installed on a computer chosen to be the management center. ***Figure 1-4*** shows a typical connection and ***Table 1-2*** shows the modules installed in each installation mode:

Installation	Software Modules
Mode One	Management Center: Root Agent + Configuration Client (Event Notification) utility
Mode Two	RAID Servers (servers A, B, and C) via in-band connections
Mode Three	RAID agents in RAID arrays (Console evoked by a browser)
Java Runtime	Required for a browser access

Table 1-2: Software Modules with Different SANWatch Installations

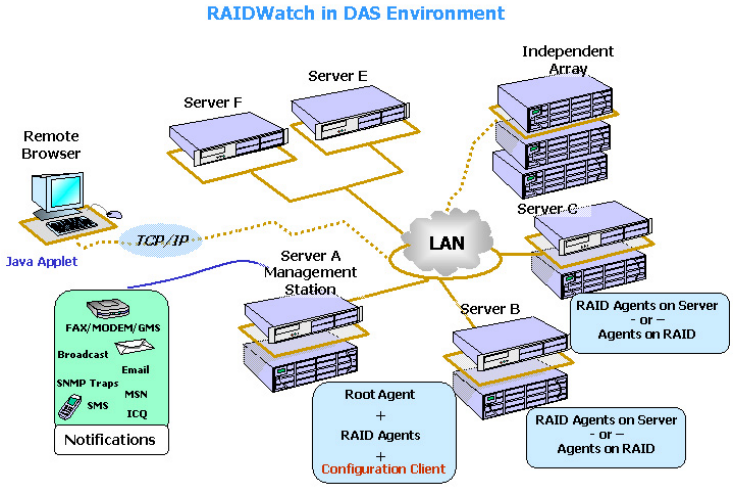


Figure 1-4: Typical SANWatch Connection – Heterogeneous

2. **Using a Workstation as the Configuration Client machine**: Applied in an environment where RAID servers are not the management stations. Access management over the network is directed through exchanges between a remote manager station and SANWatch agents that are installed to array hard drives using the Mode Three installation scheme.

   Installing the Configuration Client and Root Agent onto a management station enables Event Notification. Installing Configuration Client modules onto two or more computers can prevent chance of down time in the event of server shutdown or failure (see ***Figure 1-5***.)

Installation	Software Modules
Mode One	Management Center: Root Agent + Configuration Client utility
Mode Three	RAID agents in RAID Arrays (not necessary for JBODs)

Java Runtime	Required for a browser access

Table 1-3: Software Modules: SANWatch Console over Browser-invoked Java Applet

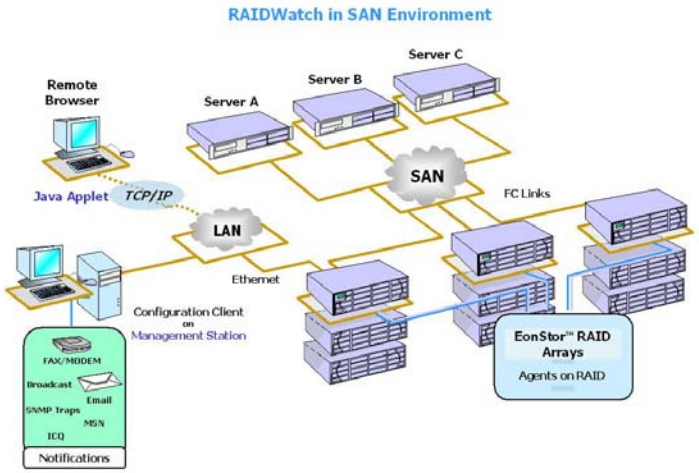


Figure 1-5: Typical SANWatch Connection – Applet Mode

3. **Stand-alone/Out-of-Band (on Subsystem) Installation:** This installation mode provides management access without the **Central Management** utility. Event notification is provided through an independent **NPC** utility. SANWatch accesses RAID subsystems over the network through the command exchanges between a manager station and SANWatch agents previously installed to array hard drives, (See ***Figure 1-6***.) The management session and the NPC configuration screen are invoked as a Java Applet.

Installation	Software Modules
Mode Three	RAID agents in RAID Array firmware
Java Runtime	Required for a browser access

Table 1-4: Software Modules: Management Only

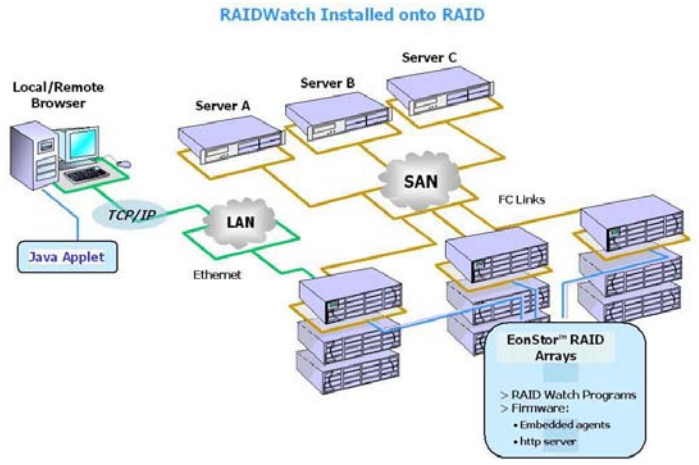


Figure 1-6: Typical SANWatch Access – the Applet Mode

1.2.5 Multi-Language Support

SANWatch is a RAID management tool widely applied all over the world. The software is currently available in four (4) languages: English, Deutsch, Spanish and Japanese. The language used in GUI is easily changed using the language selection on the main program's menu bar. As soon as a language is selected, the user interface, wizards, and online help display the chosen language.

1.2.6 Password Protection

SANWatch Manager comes with password protection to prevent unauthorized users from changing the RAID configurations. With the password security, you have control over array settings knowing that the currently managed disk array is safe from unauthorized modifications because the correct password must be entered for each access level.

The SANWatch management screen has a navigation tree panel that provides access to functional windows under three major categories:

- **Information:** An **Information** login can only access the first level, Information.
- **Maintenance:** A **Maintenance** (user) login can access the first and second levels, the Information and Maintenance tasks.
- **Configuration:** The **Configuration** (administrator) login has access rights to all three levels, Configuration, Maintenance, and Information.

NOTE:

The default password for Information (View Only) access is "**1234**."

Passwords for access levels can be set in the Configuration category under the "**Configuration Parameters**" -> "**Password**" window.

1.3 Conceptual Foundation

In order for SANWatch to function properly, different software modules must be correctly installed on different servers and stations in a given LAN or WAN. If you follow the default installation during the installation process, SANWatch will be installed as a centralized management tool into your system.

1.3.1 Centralized Management (Agent-based) Installation

1. SANWatch communicates with a RAID subsystem either using the firmware-embedded RAID agents or agents manually installed onto a RAID-attached server. Assuming that a given network has multiple RAID systems, SANWatch can communicate with RAID arrays through the RAID agents installed on the management stations or on the RAID subsystems.

2. A server is chosen as the main management server. When SANWatch is installed onto this server using the first installation scheme, two important utilities are included, **Configuration Client** and **Root Agent**. The Configuration Client enables automatic notifications of system events, and the Root Agent communicates with multiple RAID subsystems that are not directly attached to this server.

3. The main management server will also need Java Run-time Environment (JRE) installed if a system administrator needs to configure the arrays from it. The product utility CD contains a Java Run-time package.

4. ***Table 1-5*** provides a guide to what modules need to be installed on which servers.

NOTE:

The items listed in the lower section of Table 1-5, JRE, web browser and/or web server are not included with SANWatch management program; therefore, they must be manually installed or modified by system users.

5. For more information about specific platform requirements, see ***Section 3.3 Platform Requirements***.

	Mode 1 **Centralized Management**	**All Modes**	**Mode 2** **Stand-alone on Host**	**Mode 3** **Stand-alone on Subsystem**
Installed Elements	Centralized Management Server	Remote Browser Station	Server w/ RAID Directly Attached (in-band)	RAID Subsystem (Applet Mode)
Root Agent	Yes	-	-	-
RAID Agents	Yes	-	Yes	-

SANWatch Manager	Yes	-	Yes, if it is used to run SANWatch	Yes
Configuration Client	Yes	-	-	-
JRE	Yes, if it is used to run SANWatch	Yes	Yes	Yes
Web Browser	Yes	Yes	Yes	-
Web Server	Yes	-	-	Firmware-embedded

Table 1-5: SANWatch Module Requirements

1.3.2 Stand-alone (on Host) Installation

Main features of the RAID-based installation method are listed below:

- SANWatch main programs and the RAID agents used to communicate with a RAID subsystem over in-band protocols are installed.
- SANWatch runs on the RAID-attached server as a Java program.

1.3.3 Stand-alone (on Subsystem) Installation

Main features of the RAID-based installation method are listed below:

- SANWatch support2 installation to array hard drives. A portion of the drive capacity (256MB of disk space) is segregated and formatted on each hard drive. This segregated portion is called a "reserved space." Once installation begins, SANWatch's main programs are automatically transferred to the reserved space.

NOTE:

If the In-band connection to RAID arrays is used, the SANWatch program can access the arrays only when the following apply:

1. One logical drive exists and is associated with host ID/LUNs. Use the LCD keypad panel or RS-232 terminal program to create a logical drive when you are using a completely new array before installing SANWatch version 2.0 or above.
2. Another way to establish In-band connection is to configure RAID subsystems' host-side parameters settings, such as **Peripheral Device Type** and **Peripheral Device Qualifier** over a terminal emulation console.

- There is no need to install the SANWatch program to your management computer.
- If the arrays are managed by dual-redundant controllers, in the event of single controller failure, the manager interface

can "failover" to a partner controller. Operators' access to the system will not be interrupted. However, it is imperative that you connect both controllers' Ethernet ports to the network.

- The RAID subsystem can be accessed from a remote station running a web browser. SANWatch now runs in the Java Applet mode. Applet is executed when the connection is established between a remote browser and the RAID subsystem. Web browsers, which are often equipped with Java virtual machines, can interpret applets from web servers.
- The controller firmware has an embedded HTTP server. When properly configured, the controller/subsystem's Ethernet port behaves like an HTTP server.

Chapter 2

SANWatch Considerations

Before you begin installing SANWatch, the following should be considered:

- **Background Information – Section 2.1 on Page 2-2**
- **Definition of Terms – Section 2.2 on Page 2-2**
- **Operating with Spare Drives – Section 2.3 on Page 2-3**
- **Operating without Spare Drives – Section 2.4 on Page 2-3**
- **Before You Start – Section 2.5 on Page 2-4**

2.1 Background Information

Redundant Arrays of Independent Disks (RAID) is a storage technology used to improve the processing capability of storage systems. This technology is designed to provide reliability (i.e., "fault tolerance") in disk array systems and to take advantage of the performance gains by spinning multiple disks together.

RAID comes with a redundancy feature that ensures fault-tolerant, uninterrupted disk storage operations. In the event of a disk failure, disk access will still continue normally with the failure transparent to the host system.

RAID has several levels and multi-level configurations including RAID 10, 30, 50 and 60. RAID levels 1, 3 and 5 are the most commonly used levels; while the latest RAID level 6 is also available. ***Appendix C*, *RAID Levels***, gives information about these levels and the benefits of each.

Infortrend disk arrays support disk drive hot-swapping so that a failed drive can be replaced while the disk array system continues servicing I/Os. Standby spares can also be assigned so that, as soon as a drive fails, the spare is automatically configured into the array and reconstruction will commence.

2.2 Definition of Terms

This section describes some of the disk array terms used in this documentation.

- **Physical drives.** These are the actual drives installed into the enclosure drive slots. These drives are displayed in **Enclosure View** and the **Front View** of different configuration windows.

- **Spare drives.** These are physical drives that serve as backups. When a drive fails, the spare automatically joins the array and data reconstruction commences immediately. Dedicated (**Local**), **Enclosure**-specific, and **Global** Spares are shown in different colors. A Dedicated Spare appears in the same color as other members of the logical drive it belongs to. A Global Spare uses the default color (black). All types of spares have an orange cross superimposed on them.

- **Replacement drives.** These are physical drives that are manually configured into the array to replace failed drives. In the absence of spare drives, you will need to use replacement drives to replace defective drives before rebuilding. If a spare drive has been used to rebuild the array, you will also need to replace the failed drive manually to create another spare in case another drive fails. You may also apply

the "**Auto-Assign Global Spare**" feature for a new drive to automatically become a Spare drive.

- **Failed drives.** These are physical drives that fail due to some type of error. Failed drives appear with a red LED on their respective icons.

- **Logical drives.** Logical drives are the combinations of multiple physical drives. Combining physical drives into logical drives gives you a disk array with the protection of a certain RAID level. To view logical drives, select "**Existing Logical Drives**" on the navigation menu tree.

- **Logical volumes.** Volumes are the combinations of several logical drives. Combining logical drives into logical volumes gives you a single logical unit with even larger capacity. Logical volumes or their partitions are mapped to various host LUNs. To view logical volumes, select "**Existing Logical Volumes**" on the navigation menu tree.

- **Snapshot.** For terms related to Snapshot functionalities, please refer to **Chapter 15** of this manual.

2.3 Operating with Spare Drives

You can assign spare drives to a particular logical drive to serve as backup drives. When a drive fails within the logical drive, one of the spares will be automatically configured into the logical drive, and data reconstruction onto it will immediately commence.

The following are guidelines for disk failure recovery when a spare drive is available:

- If a spare drive exists in the same logical drive, the controller will automatically mount the spare drive and start rebuilding data in the background.

- Depending on system design, it may be possible to remove a defective drive and replace it with a new drive without shutting down the system (hot-swapping). All EonStor subsystems support drive hot-swapping.

- The replacement drive must then be assigned as a new spare drive. You may also enable the "**Auto-Assign Global Spare**" feature for a new drive to be automatically configured into a Global Spare.

2.4 Operating without Spare Drives

The following are guidelines for disk failure recovery when a spare drive is not available:

- Depending on the design of the system, it may be possible to remove a defective drive and replace it with a new drive without shutting down the system (hot-swapping). All EonStor subsystems support drive hot-swapping.

- If the replacement drive is installed on the same channel and ID (the original drive slot where the faulty drive was), you can then proceed with data rebuilding by checking the rebuild command in the logical drive status window.

- If the replacement drive is installed on a different channel or using a different ID (different drive slot) or the "periodic drive scan" function has been disabled, you need to scan in the new drive first (SCSI bus), and then assign it as a spare drive of the logical drive which had a drive failure. Data rebuilding will have to be manually initiated.

IMPORTANT!

Although the RAID system provides uninterrupted disk access even after a disk failure, do not leave a failed drive unattended. Without a replacement, the system will not survive a second physical drive failure on the same logical drive (RAID3 and 5). A defective drive must be promptly replaced and data rebuilt.

CAUTION!

When performing hot-swapping, be sure to remove only the defective drive. Removing the wrong drive will result in complete, irrecoverable data loss. Use the **Enclosure View** window or **Logical Drive Information** window to locate exactly which physical drive has failed.

2.5 Before You Start

SANWatch Manager comes with password protection that prevents unauthorized modification of the disk array configuration. During each attempt at modifying the system configuration, the configuration will require the correct password before proceeding.

By default, the SANWatch Manager station comes with a password, "**1234**," for login as an **Information** viewer. The password required for the "**Configuration**" level access is identical to that configured through the firmware utility for each RAID subsystem. For information on how to set a password and other security features, see the ***Password*** section of ***Chapter 7***, ***Configuration Parameters***.

Chapter 3
Installation

This chapter describes SANWatch requirements and the installation procedure. The following sections are covered in this chapter:

- **System Requirements – Section 3.1, page 3-2**
  - **3.1.1 Servers Running SANWatch**
  - **3.1.2 Local Client Running SANWatch Manager**
- **RAID Chart – Section 3.2, page 3-4**
- **Platform Requirements – Section 3.3, page 3-5**
- **Software Setup – Section 3.4, page 3-6**
  - **3.4.1 Before You Start**
  - **3.4.2 Installing SANWatch on a Windows Platform**
  - **3.4.3 Installing SANWatch on a Linux Platform**
  - **3.4.4 Installing SANWatch on a Solaris Platform**
  - **3.4.5 Installing SANWatch on a Mac OS running Safari Browser**
  - **3.4.6 Installing SANWatch**
  - **3.4.7 Installing Software Components**
  - **Stand-alone (on Host or Subsystem) Installation**
- **Using Snapshot (Data Service)**
- **Program Updates – Section 3.5, page 3-21**
- **In-band SCSI – Section 3.7, page 3-23**
  - **3.7.1 Overview**
  - **3.7.2 Related Configuration on Controller/Subsystem**

3.1 System Requirements

The minimum hardware and software requirements for SANWatch are listed below.

3.1.1 Servers Running SANWatch

A server can be chosen as the Centralized Management center, which uses the **Configuration Client** and **Central Management** utilities and can be installed with the SANWatch manager program using the first installation scheme (Centralized Management) in the **Custom Mode**.

- Computer must be Pentium or above PC-compatible running

  - Windows 2003 R2 sp1 (32/64), Windows XP, Vista

  - RedHat AS 3.0, ES 4 (32/64),

  - SUSE Linux Enterprise 9 (64), Professional 9.1, SLES 10 (32/64)

  - Fedora Linux 3 (64), Fedora Linux 5 (32/64)

  - FreeBSD 5

  - Solaris 9/10 Sparc

  - Mac OS X 10.4.x

  All above OSes should support Java Runtime 1.4.2_05 or higher.

- The **Data Service**, Snapshot function currently supports Windows Server 2003 R2 SP2 32-bit and Server 2003 SP2 64-bit platforms.

NOTE:

1. The optimal configuration for running the Data Service functionality in SANWatch is listed below:

   RAID controller **caching mode**: write-back

   Disk buffer: disabled

   BBU protection: enabled

   BBU **Event–triggered operation**: enabled

   If your current firmware configuration does not match the above, when you activate Data Service the above preferences will automatically apply.

2. The On **Linux** 64-bit Enterprise 4, a shell command can facilitate **In-band** connection: "MODPROBE sh". Connection will be validated after the RAID/Root agent is re-activated.

- 16K or higher mode management station monitor.
- At least one available Ethernet port is required (over TCP/IP).
- **Data Service** (Snapshot) Application support:

  Windows Server 2003 R2 SP2 32-bit and Server 2003 SP2 64-bit

  Service: Microsoft VSS: Application-aware snapshot capabilities (shadow copies) with hardware provider

3.1.2 Local Client Running SANWatch Manager (the RAID Management Part)

- Computer must be Pentium or above PC-compatible running
  - Windows 2003 R2 sp1 (32/64), Windows XP, Vista
  - RedHat AS 3.0, ES 4 (32/64),
  - SUSE Linux Enterprise 9 (64), Professional 9.1, SLES 10 (32/64)
  - Fedora Linux 3 (64), Fedora Linux 5 (32/64)
  - FreeBSD 5
  - Solaris 9/10 Sparc
  - Mac OS X 10.4.x

  All above OSes should support Java Runtime 1.4.2_05 or higher.
- The **Data Service** (Snapshot) functions currently support Windows 2003 platforms.

NOTE:

Java Runtime consumes additional memory and resources. A memory size of **512MB** or more is preferred on your management computer if you need to open more than one SANWatch console with multiple RAID systems.

- Remote station must be running Netscape 4.7X, IE6.0 or Mozilla 5.0, Java Runtime 1.4.2_05 (for a particular platform).
- 16K or higher mode management station monitor.
- One Ethernet port (over TCP/IP)

- Windows Messaging (MAPI) for Windows 2003/XP if fax notification support is needed.

- Windows NetBEUI support for Windows 2003/XP must be enabled if network broadcast support notification is needed. Please refer to your Windows documentation for more information.

- SNMP traps service for Windows NT if SNMP traps notification is desired.

- TCP/IP with a valid IP assigned to each controller/subsystem. Static IP is recommended.

- A fax modem that supports Hayes AT command protocol is required (if using the fax event notification function.) (Fax command class 2.0 and above.)

- A GSM modem is required (if using the SMS short message event notification function). SANWatch currently supports two GSM modem models:

  - Siemens TC35
  - WAVECOM Fast Rack M1206

NOTE:

Please contact Infortrend for the complete list of compatible GSM modems.

3.2 RAID Chart

Before installing SANWatch and its various agents and modules, it is helpful to chart your RAID subsystems. If you operate a single RAID subsystem from a local or remote workstation, you may skip this section. If you have multiple RAID subsystems, the information shown in ***Table 3-1*** provides guidelines for charting existing RAID subsystems. Each field is explained as follows:

RAID System	RAID System 1	RAID System 2	RAID System 3	RAID System 4
ID/Name	Example	Example	Example	….
Location	HQ	Installation site	Storage	….
OS	Windows 2003	Windows 2003	N/A	….
IP Address	205.163.164.111	205.124.155.102	xxx.xxx.xxx.xxx	….
Role	Centralized Management Center	Root Agent (Intermediate SANWatch	RAID Agent (RAID Storage)	….

		station)		
Internet Capable	Yes	Yes	Yes	….
Table 3-1: RAID Charting Table				

- **ID/Name:** User designated; an ID or name should be a unique identifying label.
- **Location:** A specific geographic reference (e.g., headquarters, Building 3, Equipment Room 100.)
- **OS:** The Operating System running on the particular system.
- **IP Address:** If available.
- **Role:** The purpose fulfilled by the particular system, relative to RAID operations.
- **Internet Capable:** If a server is an Internet server, the answer to this is "***Yes***." If a workstation will manage RAID systems through a browser, note the particular browser software, its version number, and its support for Java.

3.3 Platform Requirements

SANWatch supports various operating systems both for servers (RAID management hosts or web servers) and for client management stations (SANWatch Manager workstations). Support for Java, however, depends on the Java Runtime installed on each OS. Below are the platform requirements using windows OSes.

1. Under Windows 2003, the Java installation program, installshield.jar, ONLY supports:
   - Netscape 4.5 (or above)
   - Microsoft Internet Explorer 4.0 (or above)
2. Windows Messaging (MAPI) for Windows must be enabled if support for fax or email notification under NT is needed. Refer to your Windows documentation for more information.
3. Windows NetBEUI support for Windows must be enabled if network broadcast support notification is needed. Refer to your Windows documentation for more information.

3.4 Software Setup

This section discusses how to install SANWatch in your system. Before proceeding with the setup procedure, read through the ***Before You Start*** section below. The sections follow will explain how to install SANWatch in different operation systems.

3.4.1 Before You Start

Before starting the installation, read through the notes listed below:

- TCP/IP must be installed and running with a valid IP address assigned to a server. The server can either be used as a centralized management station, a remote client using a browser to access the array, or directly attached with a RAID subsystem using the in-band protocols.
- Your system display must be running in 16K colors or higher mode otherwise some configuration items may not be visible.
- Be certain that your system meets the minimum hardware and software requirements listed in ***Section 3.1 System Requirements***.
- Check to confirm that the RAID disk arrays and controllers are installed properly. For the installation procedure, see the documentation that came with the controller/subsystems.
- Follow the directions provided in the ***Section 3.3 Platform Requirements,*** and prepare for installation and operation under different OS environments.

3.4.2 Installing SANWatch on a Windows Platform

If you are running a Windows platform on the server computer follow these steps to install SANWatch on your server(s) and RAID subsystem:

Step 1. Insert the Infortrend Product Utility CD or SANWatch installation CD into the system's optical drive.

Step 2. If you are currently running other applications, close them before proceeding with the setup process. This will minimize the possibility of encountering system errors during setup.

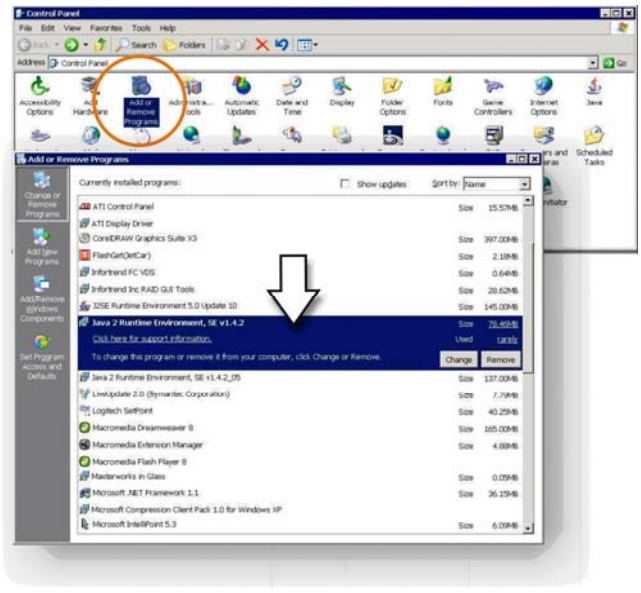
Step 3. The SANWatch installer program is included on the CD-ROM that came with your RAID controller or subsystem. An auto-run screen provides a hot link to the Windows installer program. Click on "**Windows Platform**."

Step 4. Click the supported platform to start the installation process.

Step 5. If your server or workstation is not ready with Java Runtime (at least version 1.4.2_05), an install shield will automatically install Java Runtime onto your machine. Please follow the on-screen instructions to proceed.

NOTE:

It is best to remove older Runtime packages from your machine. The older Java Runtime can be removed through (Windows platform) the "**Control Panel**" -> "**Add or Remove Programs**" utility.



Step 6. To install the Java-based GUI SANWatch manager main program, see ***Section 3.4.6*** for detailed procedures.

3.4.3 Installing SANWatch on a Linux Platform

If you are running a Linux platform on the server computer follow these steps to install SANWatch on your server(s):

Step 1. Insert the Infortrend Product Utility CD or SANWatch installation CD into the system's optical drive.

Step 2. If you are currently running other applications, close them before proceeding with the setup process. This will minimize the possibility of encountering system errors during setup.

Step 3. Open the file manager and change the directory to /mnt/cdrom.

Step 4. Locate and execute ./linux.sh to start the software installation.

Step 5. Be sure to install JRE 1.4.2_05 or above version on your server. Running older version of Java runtime may cause a failure of installing SANWatch main program.

Step 6. Be sure to install the Java plug-in.

Step 7. Install the Java-based GUI SANWatch manager main program. An installshield will prompt on the screen. Please refer to ***Section 3.4.6*** for step-by-step installation procedures.

3.4.4 Installing SANWatch on a Solaris Platform

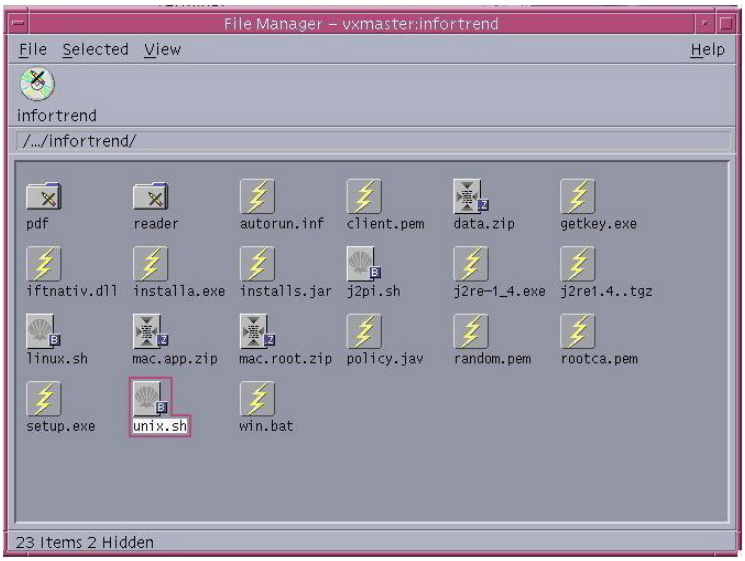
Follow these steps to install SANWatch on your server(s) and RAID subsystems:

Step 1. Insert the Infortrend Product Utility CD or SANWatch installation CD into the systems CD-ROM drive.

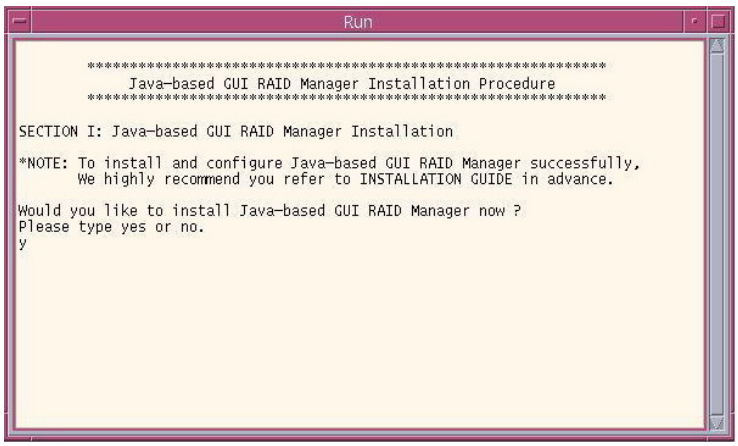
Step 2. If you are currently running other applications, close them before proceeding with the setup process. This will minimize the possibility of encountering system errors during setup.

Step 3. Be sure to install JRE 1.4.2 or above version on your server. Running older version of Java runtime may cause a failure of the SANWatch main program installation.

Step 4. When the **File Manager** window pops up on the screen, double-click the file "unix.sh."



Step 5. A **Run** window prompt will display. To install the Java-based GUI SANWatch manager main program, type **YES** and then press **Enter**. This will launch SANWatch manager install shield. Please refer to ***Section 3.4.6*** for step-by-step installation procedures.


Run
Java-based GUI RAID Manager Installation Procedure
SECTION I: Java-based GUI RAID Manager Installation
*NOTE: To install and configure Java-based GUI RAID Manager successfully,
We highly recommend you refer to INSTALLATION GUIDE in advance.
Would you like to install Java-based GUI RAID Manager now ?
Please type yes or no.
y

3.4.5 Installing SANWatch on a Mac OS Running Safari Browser

Enabling Root Access

SANWatch installation onto a Macintosh machine running Safari browser requires you to enable the root account first. The Mac OS ships with the root account disabled as an intentional security feature to avoid problems that could arise from casual use of root access.

Enabling/Disabling the root access requires administrative privileges. You will need to know the password for the "Admin" account first. If the Admin password is not available, you may reboot from an installation CD and find the menu item for "Password Reset."

NOTE:

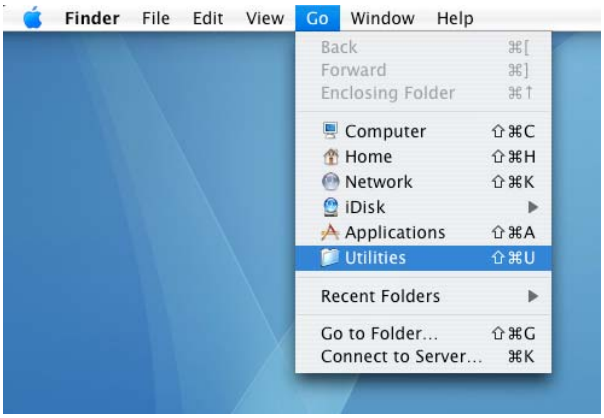
You may temporarily disconnect your Mac machine from the network during the time you use the root account to complete specific configuration task. Unauthorized access during the time can cause problems to your OS.

Remember to re-connect the cabling after SANWatch installation.

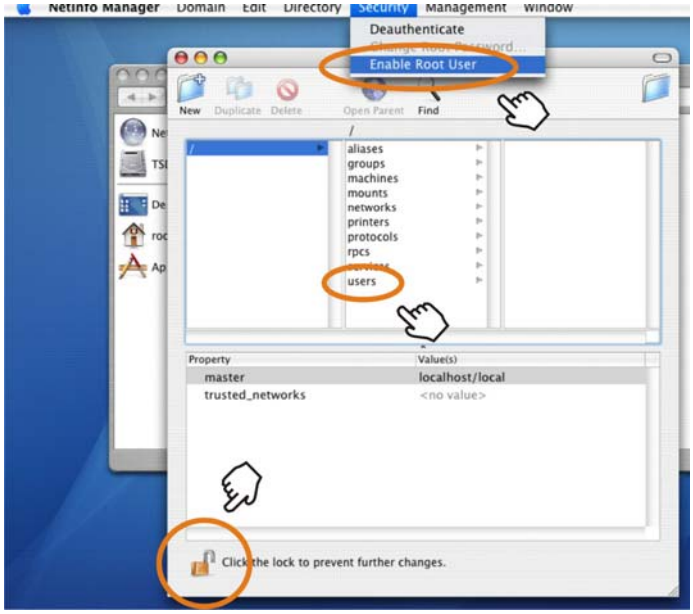
To enable the **root access**:

Step 1. Login in using the Admin account.

Step 2. Locate the **GO** menu from Mac OS X's finder menu bar, access the "**Utilities**" folder to start the "**NetInfo Manager**" application.



Step 3. Click on the "**Lock**" icon on the lower left of the screen before you make configuration changes.



Step 4 Locate the "**Security**" item from the top menu bar. Select "**Enable root user**." You will have to enter the administrator's password to authenticate yourself.

Step 5. From this screen you can also enter a new password for root access. Select "**users**" in the middle column (as shown in the diagram above). Provide the administrative password as prompted.

Find the "**password**" field, click on the value field to alter it (it should contain just the "*****" as an encrypted password). Double-click and then enter a new password. Make sure there are no spaces left in the value field.

Step 6. Log out and log in as the "root" user to verify that it worked. Select "Other" from the login screen and manually enter "root" as user name and its associated password.

Step 7. When you log in successfully, you can start installing SANWatch to your Mac machine.

Running the Configuration Client and Central Management utilities requires you to log in as a root user. In-band drivers also require root access.

If you do not need the Configuration Client and Central Management utilities and run the SANWatch management software over the Applet mode, you may log in using your ordinary user access.

The Install Shield

To install SANWatch package for Mac OS, simply locate the installation files and double-click the "**installshield.jar**" to start with the installation process.

3.4.6 Installing SANWatch Main Program (for all platforms)

When the install shield of SANWatch main program is launched, follow the steps below to complete the installation.

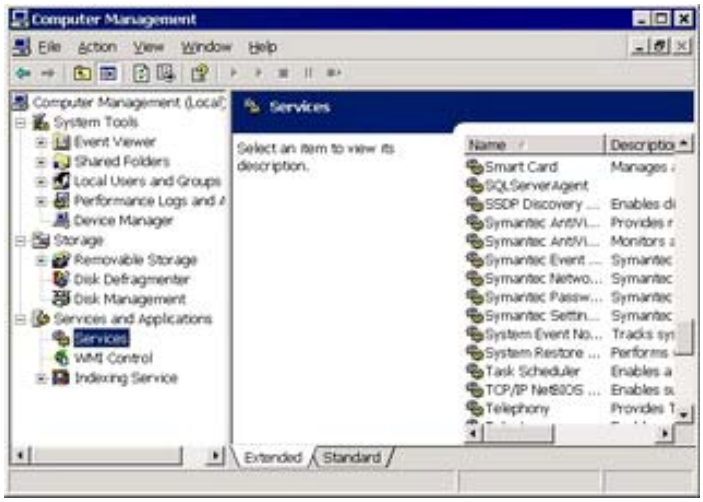
IMPORTANT!

It is recommended to uninstall previous Infortrend software, e.g., RAIDWatch, before installing SANWatch.

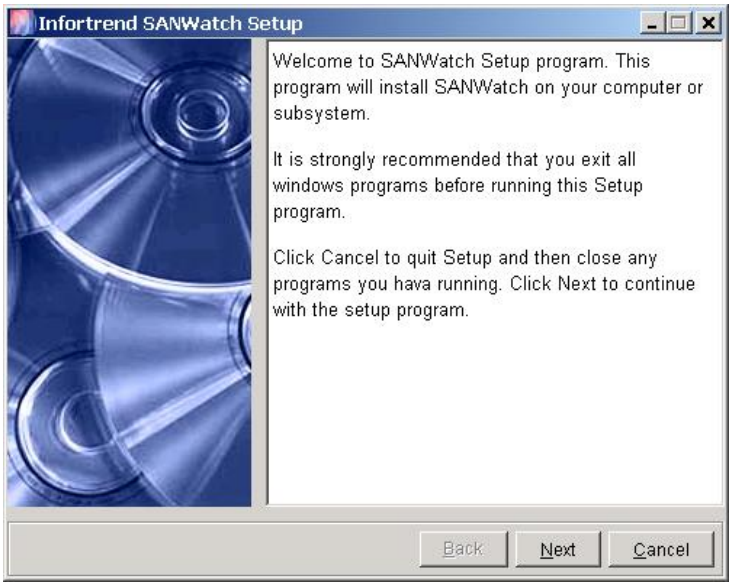
It is also necessary to **reboot** your system to complete the uninstallation

process.

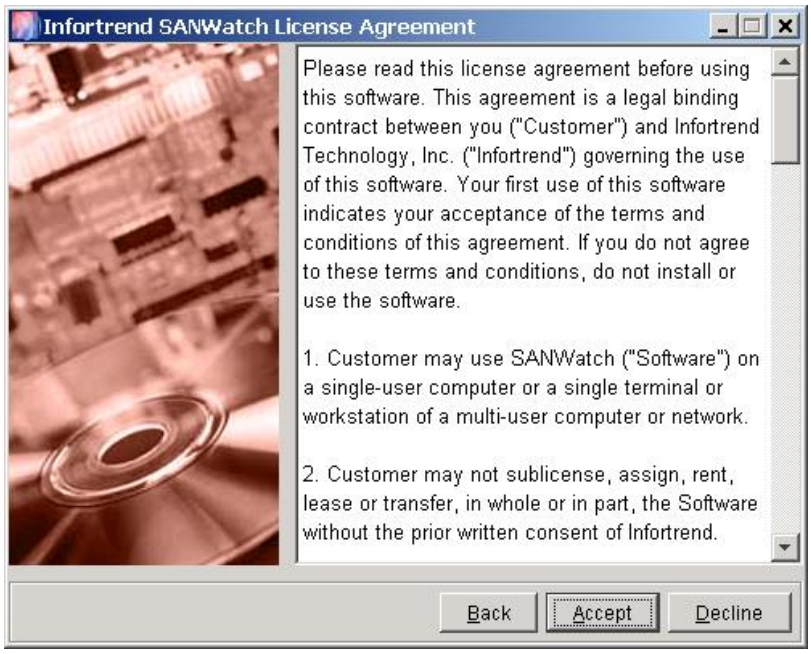
Before installing SANWatch, it is also a good practice to check if the previous version of **RAID agents** are evoked. For example, on a Windows platform you can check in the **Computer Management** utility -> **Services and Applications** -> **Services**. You should then disable the previous version of RAID agents.



Step 1. To install SANWatch, click the ***Next*** button at the bottom of the window. If you do not wish to continue with the installation process, select the ***Cancel*** button.


Infortrend SANWatch Setup
Welcome to SANWatch Setup program. This program will install SANWatch on your computer or subsystem.
It is strongly recommended that you exit all windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you hava running. Click Next to continue with the setup program.
Back
Next
Cancel

Step 2. If you selected the ***Next*** button, the License Agreement window shown below will appear. First read through the License Agreement. If you are in agreement with the specified terms and wish to continue installing the SANWatch program, select ***Accept***. If you do not wish to continue with the installation process then select the ***Decline*** button.

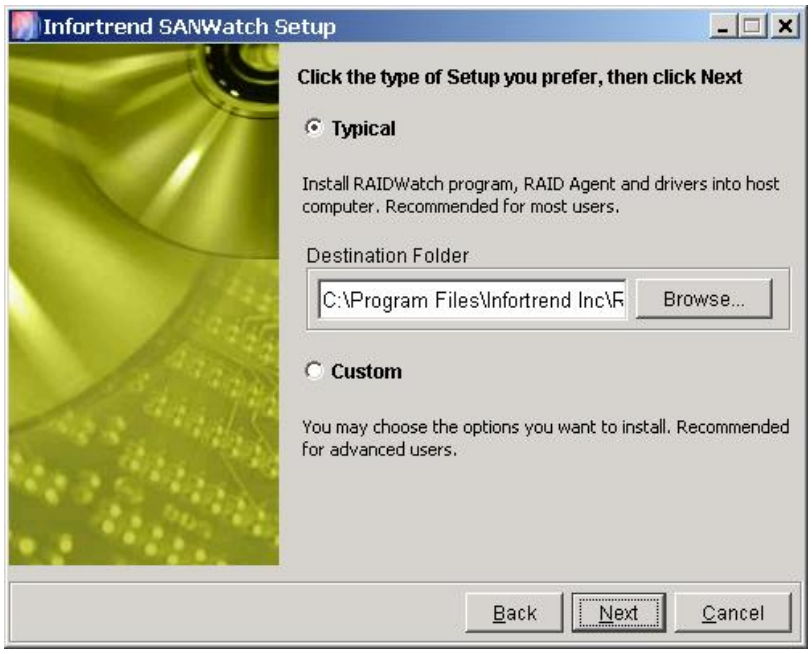

Infortrend SANWatch License Agreement
Please read this license agreement before using this software. This agreement is a legal binding contract between you ("Customer") and Infortrend Technology, Inc. ("Infortrend") governing the use of this software. Your first use of this software indicates your acceptance of the terms and conditions of this agreement. If you do not agree to these terms and conditions, do not install or use the software.
1. Customer may use SANWatch ("Software") on a single-user computer or a single terminal or workstation of a multi-user computer or network.
2. Customer may not sublicense, assign, rent, lease or transfer, in whole or in part, the Software without the prior written consent of Infortrend.
Back
Accept
Decline

Step 3. If you accepted the License Agreement, a new window with two installation options will appear. These options are **Typical Install** and **Custom Install**. The default is set to **Basic Install**. All users are recommended to install SANWatch program using the default settings. This will create a new "Infortrend Inc" folder on the computer chosen as a management center. If you want to install SANWatch in a different folder, type in a new location or click the ***Browse*** button to select a destination folder. If you follow the default selection and click the ***Next*** button, the install shield will start install the SANWatch software, RAID Agents, and necessary drivers on the computer.

If you want to install the management utility redundantly onto two different servers, select **Advanced Install**, and click the ***Next*** button to choose a desired installation mode in the next screens.

NOTE:

To properly install the new Central Management utility, please install SANWatch using the "**Custom**" -> "**Centralized Management**" setting.


Infortrend SANWatch Setup
Click the type of Setup you prefer, then click Next
Typical
Install RAIDWatch program, RAID Agent and drivers into host computer. Recommended for most users.
Destination Folder
C:\Program Files\Infortrend Inc\F
Browse...
Custom
You may choose the options you want to install. Recommended for advanced users.
Back
Next
Cancel

Step 4. If you choose the **Custom** installation mode on the previous screen, three (3) installation modes will appear in the following screen. These modes are **Centralized Management**, **Stand-alone (on Host)**, and **Stand-alone (on Subsystem)**.

- **Centralized Management** – Selecting this option allows you to install the complete software utilities including the SANWatch software, a Root Agent, RAID Agents, Configuration Client utility, and necessary drivers on the computer chosen as a management center.

  The new Central Management utility is also installed in this process. The utility provides Online monitoring of multiple RAID subsystems across the network.

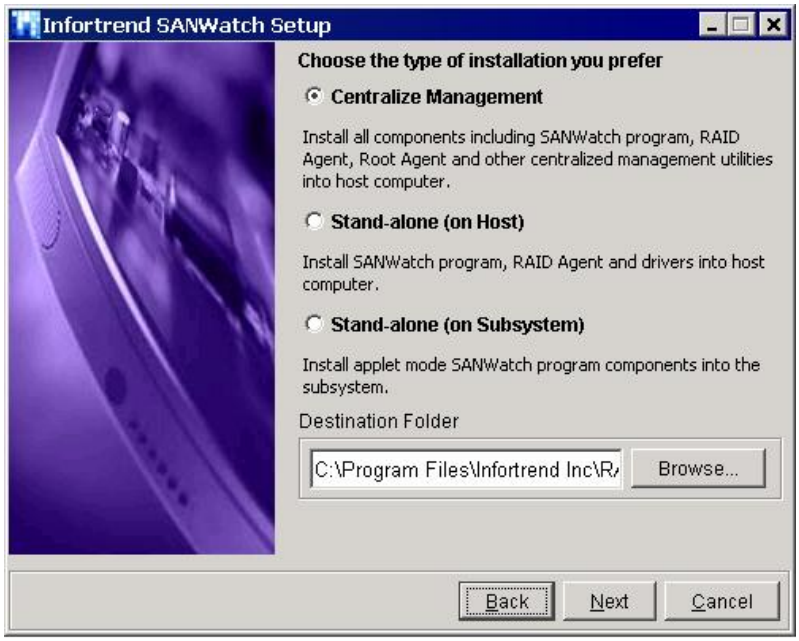
- **Stand-alone (on Host)** – Selecting this option will install the In-band driver (RAID agents) for servers that are directly attached to a RAID subsystem, and the SANWatch software on the local host.

- **Stand-alone (on Subsystem)** – This will install the software onto the controller/subsystem itself. The EonStor subsystems come with necessary RAID agents embedded in the firmware. A RAID subsystem will use a small section of formatted disk space (called the reserved space) to store software related files. Installed in this mode, SANWatch can be started by a remote browser accessing the array through the subsystem's Ethernet port (via a pre-assigned IP).

If the **Stand-alone** (**on Subsystem**) installation was selected, you will have to use a web browser to connect to the SANWatch program. To do this, open a web browser and enter the controller/subsystem IP address.

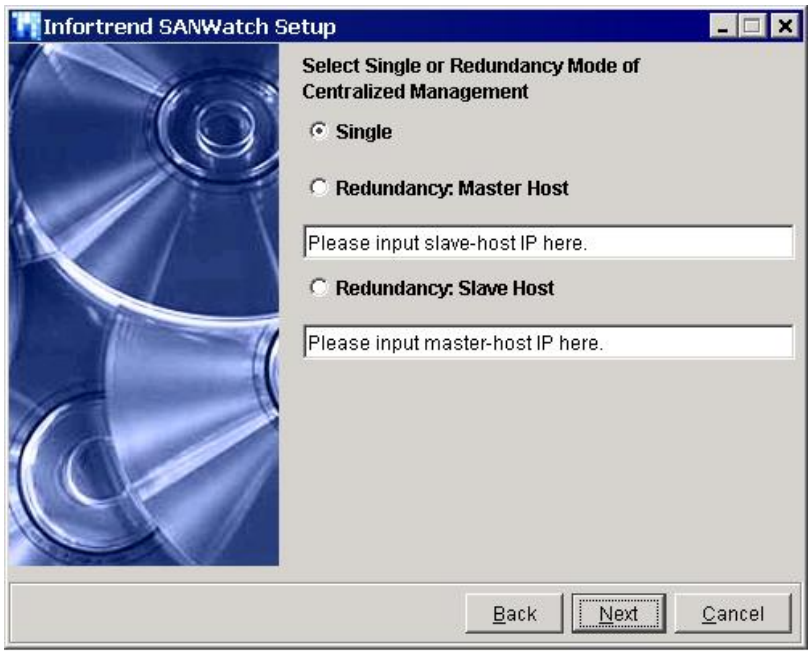
IMPORTANT!

There is no need to configure the Peripheral Device setting if you are trying to manage a RAID subsystem from a SANWatch station through an Ethernet connection (to the EonStor subsystem's Ethernet port). An Ethernet connection to RAID uses TCP/IP as the communication protocol.

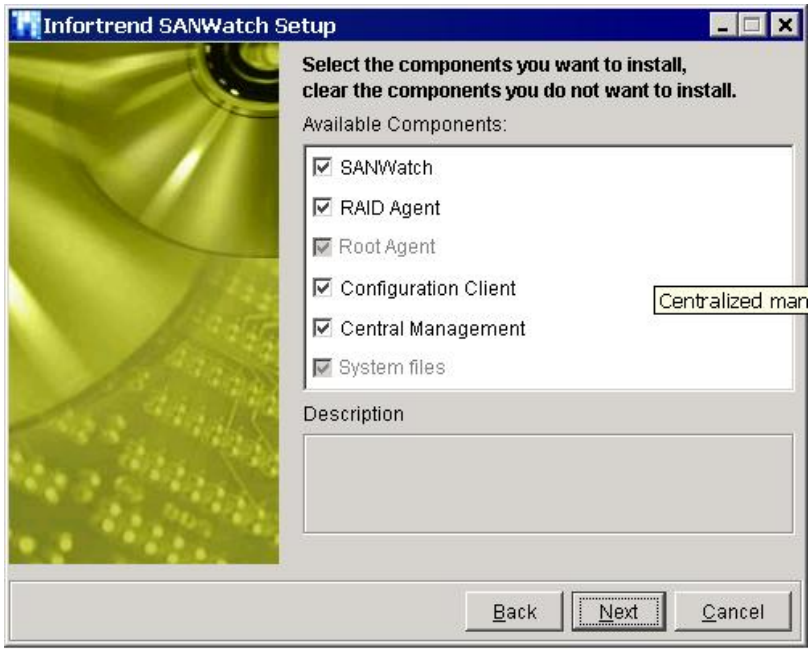

Infortrend SANWatch Setup
Choose the type of installation you prefer
Centralize Management
Install all components including SANWatch program, RAID Agent, Root Agent and other centralized management utilities into host computer.
Stand-alone (on Host)
Install SANWatch program, RAID Agent and drivers into host computer.
Stand-alone (on Subsystem)
Install applet mode SANWatch program components into the subsystem.
Destination Folder
C:\Program Files\Infortrend Inc\R
Browse...
Back
Next
Cancel

3.4.7 Installing Software Components

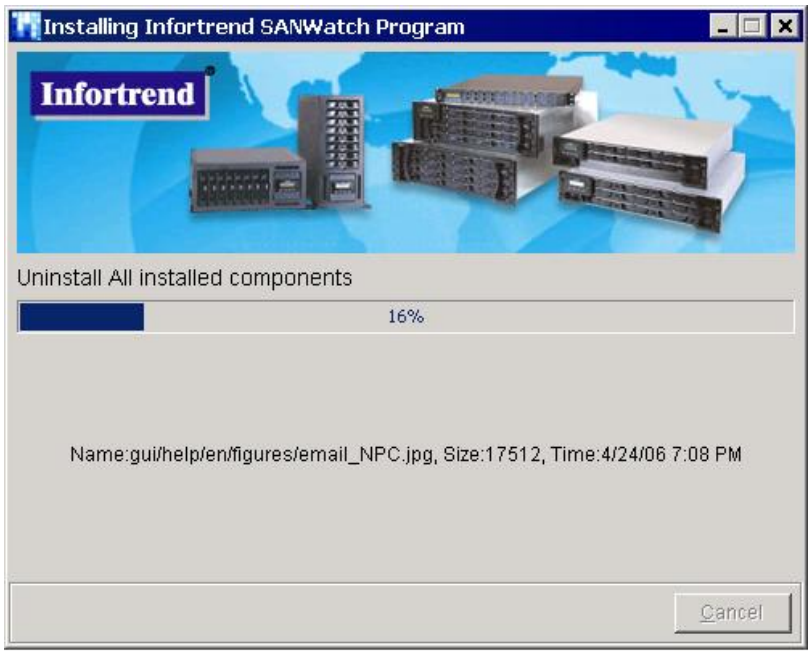
SANWatch allows you to install its management utility redundantly onto two different servers. This prevents blind time if one server fails or is powered down for unexpected reasons. Note that if another server is chosen as either the Master or Slave host, SANWatch must be manually installed on it.



Step 1. SANWatch allows you to select components during the **Custom** installation process. However, it is recommended to keep all the default combinations.



Step 2. Once the components that you want have been selected, select the ***Next*** button to proceed with the installation. If you do not wish to proceed with the installation process, select the **Cancel** button. If you wish to re-select the installation options, select the **Back** button.



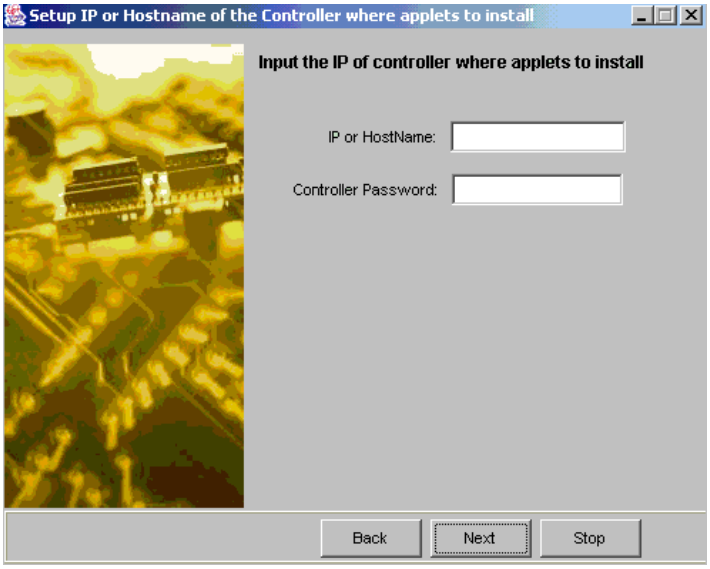
Step 3. If the **Next** button was selected, the Installation Progress window appears. If you wish to stop the installation procedure, click the **Cancel** button.

Step 4. Once the software has been successfully installed, a window indicating the successful installation will appear. To complete the process and exit the window, click on the **Finish** button. Another Windows message will prompt reminding you to reboot your system to complete the installation process. You should click **No**, locate and click on the **Finish** button on SANWatch's installer screen, and then reboot your system later.

System Settings Change
You must restart your computer before the new settings will take effect.
Do you want to restart your computer now?
Yes
No

Installing Infortrend SANWatch Program
Infortrend
Installation has completed.
The SANWatch program was installed successfully on your computer.
Click Finish to exit the setup window.
Finish

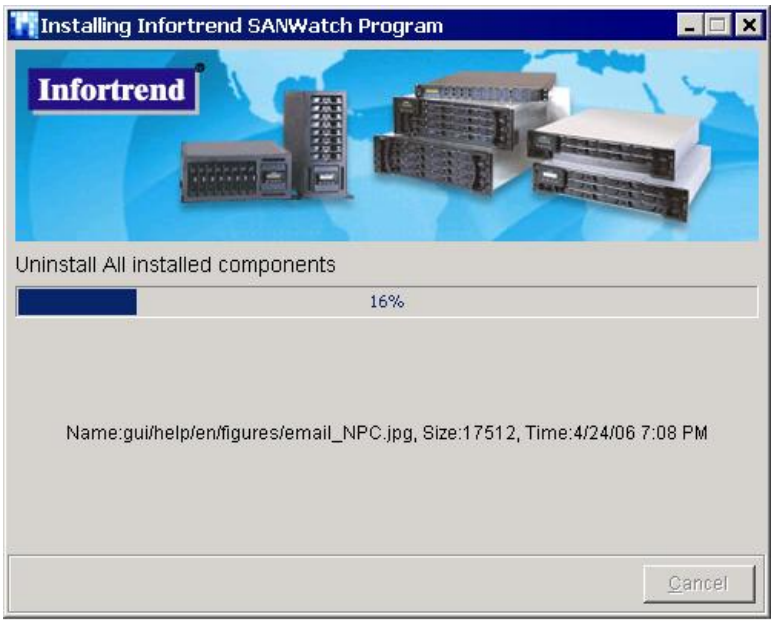
3.4.8 Stand-alone (on Host or Subsystem) Installation


Setup IP or Hostname of the Controller where applets to install
Input the IP of controller where applets to install
IP or HostName:
Controller Password:
Back
Next
Stop

Step 1. As shown above, enter the IP address or the host name of the RAID controller/subsystem and the controller password in their respective fields. The default for the controller/subsystem IP or password is blank. The preset IP and password should have been properly configured using other configuration utilities before proceeding with the SANWatch installation.

Once the IP (or host name) and the controller password have been entered, click on the ***Next*** button. If you do not wish to proceed with the installation process, select the ***Stop*** button. If

you wish to re-select the installation options, then select the ***Back*** button.



Step 2. If the ***Next*** button was selected, the Installation Progress window will appear. If you wish to stop the installation procedure, then click the ***Cancel*** button.

Step 3. Once the software has been successfully installed, a window indicating the successful installation will appear. To complete the process and exit the window, click the ***Finish*** button.

Installing Infortrend SANWatch Program
Infortrend
Installation has completed.
The SANWatch program was installed successfully on your computer.
Click Finish to exit the setup window.
Finish

Step 4. If you wish to immediately access the SANWatch manager, open a web browser and provide the IP address of your RAID subsystem. If using the in-band connection, your SANWatch

manager should directly open the console with the directly-attached RAID subsystem.

To run the **SANWatch Manager** from the controller, enter the following into the address bar of the web browser:

http://www.xxx.yyy.zzz

where **www.xxx.yyy.zzz** is the IP address entered during the installation steps.

3.5 Using Snapshot (Data Service)

IMPORTANT!

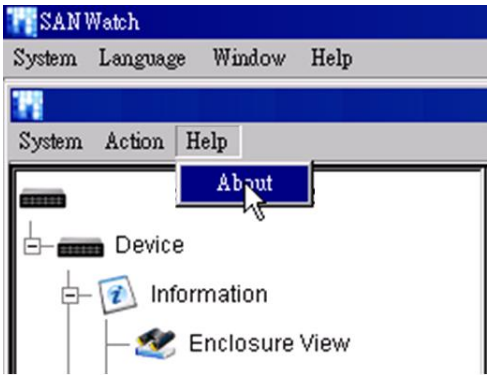
A Professional version of 30-day trail use is available with or without downloading the license key. See the below description for how to activate the trial use.

A licensed login requires:

1. At least a 512MB cache in your RAID subsystem (on each RAID controller).
2. Purchasing SANWatch by the following license application procedure.
3. A corresponding firmware version with the support for functionalities such as snapshot.

The **Data Service** (Snapshot) functionality will not be available unless the 30-day trial use is manually activated in the following way:

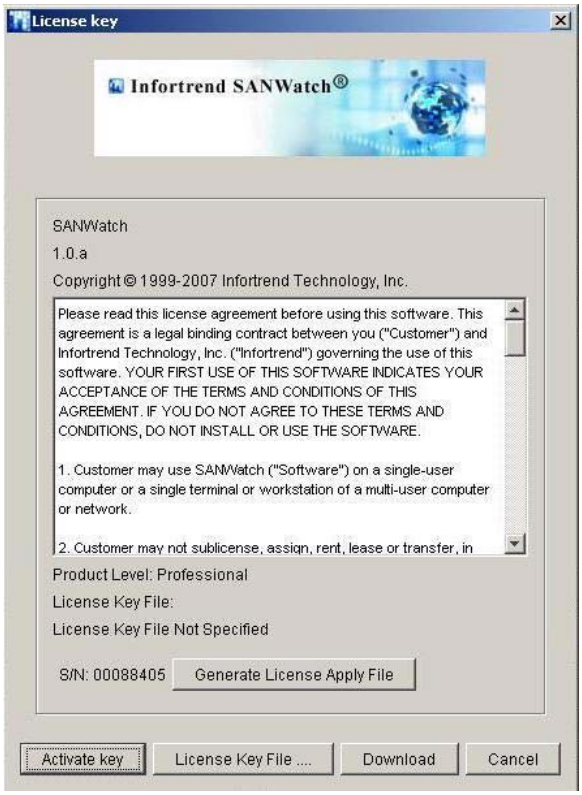
Click on the **About** button on the **Help** menu of the array management window (not the outer shell window).



Trial Use:

Click on the **Activate Key** button to begin the 30 days trial use of the software. The trial use of snapshot functionality also requires resetting your RAID subsystem.

If you are running older firmware such as FW3.48, you should upgrade your firmware and use the **Generate License Apply File** button to produce an **Apply File**. Submit the file to your vendor or log in our VIP room website to apply a trial use. For more information, please refer to **Chapter 15**.


License key
Infortrend SANWatch®
SANWatch
1.0.a
Copyright © 1999-2007 Infortrend Technology, Inc.
Please read this license agreement before using this software. This agreement is a legal binding contract between you ("Customer") and Infortrend Technology, Inc. ("Infortrend") governing the use of this software. YOUR FIRST USE OF THIS SOFTWARE INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT INSTALL OR USE THE SOFTWARE.
1. Customer may use SANWatch ("Software") on a single-user computer or a single terminal or workstation of a multi-user computer or network.
2. Customer may not sublicense, assign, rent, lease or transfer, in
Product Level: Professional
License Key File:
License Key File Not Specified
S/N: 00088405
Generate License Apply File
Activate key
License Key File ....
Download
Cancel

3.6 Program Updates

As Infortrend's valued customer, you are entitled to free program updates. You can download the latest version of SANWatch from Infortrend's FTP sites at *ftp.infortrend.com.tw* or the esupport websites. For customers granted special access, the update files can also be found in the VIP section of Infortrend's website. For more information about this service, contact Infortrend support or an Infortrend distributor in your area.

3.7 In-band SCSI

3.7.1 Overview

To meet the needs of device monitoring and administration, more and more external devices require communication with the host computers. Out-of-band connections such as an Ethernet port can be used to achieve this goal.

An alternative way of communication is in-band SCSI, which transfers configuration commands into supported SCSI commands and uses them to communicate with RAID arrays over the existing SCSI or Fibre host connections. The traditional way for controllers to communicate with the host computer has been via software (such as SANWatch) using an Ethernet connection. With in-band commands, integrators have more flexibility and may use the existing host connection instead.

There are limitations on the use of in-band protocols. For example, in order for a host to "see" the RAID controller/subsystem, at least one (1) logical drive must exist and be associated with host ID/LUNs. Otherwise, the RAID controller/subsystem itself must be configured to appear as a peripheral device to the host computers.

See the examples below for the procedures on configuring RAID controller/subsystems into a peripheral device.

3.7.2 Related Configuration on Controller/Subsystem

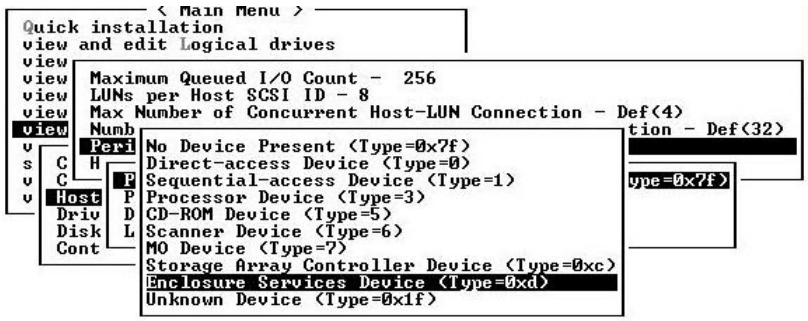
The RAID controller or subsystem must make some adjustments as well as the host computer's SNMP settings before the two can communicate using SCSI commands. You can use the RS-232 terminal utility to change the RAID controller settings.

Step 1. From the **Main** Menu, press the ***Up*** or ***Down*** buttons to select "**View and Edit Configuration Parameters**."

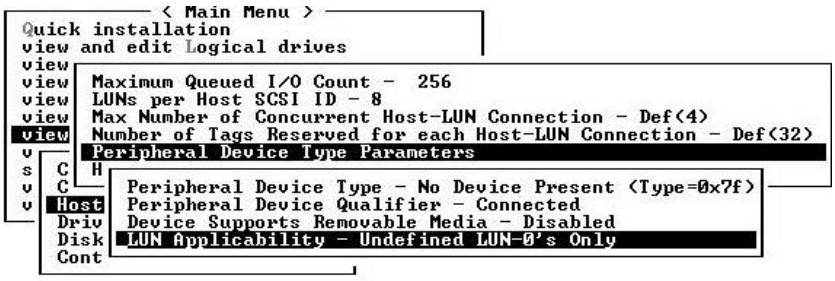
Step 2. Press ***Enter***; and then use the ***Up*** or ***Down*** keys to select "**Host-side SCSI Parameters**." Then press ***Enter***.

The **Peripheral Device Type Parameters** submenu also needs to be adjusted. Refer to the instructions below to set the proper settings for the in-band protocol to work.

Step 1. First select the "**Peripheral Device Type**" submenu and then select "**Enclosure Services Devices <Type=0xd>**."


< Main Menu >
Quick installation
view and edit Logical drives
Maximum Queued I/O Count - 256
LUNs per Host SCSI ID - 8
Max Number of Concurrent Host-LUN Connection - Def(4)
No Device Present (Type=0x7f)
Direct-access Device (Type=0)
Sequential-access Device (Type=1)
Processor Device (Type=3)
CD-ROM Device (Type=5)
Scanner Device (Type=6)
MO Device (Type=7)
Storage Array Controller Device (Type=0xc)
Enclosure Services Device (Type=0xd)
Unknown Device (Type=0x1f)

Step 2. Select "**LUN Applicability - Undefined LUN-0's Only**" option.


< Main Menu >
Quick installation
view and edit Logical drives
Maximum Queued I/O Count - 256
LUNs per Host SCSI ID - 8
Max Number of Concurrent Host-LUN Connection - Def(4)
Number of Tags Reserved for each Host-LUN Connection - Def(32)
Peripheral Device Type Parameters
Peripheral Device Type - No Device Present (Type=0x7f)
Peripheral Device Qualifier - Connected
Device Supports Removable Media - Disabled
LUN Applicability - Undefined LUN-0's Only

Step 3. Leave other options at their defaults. In-band should work fine by setting these two options.

NOTE:

1. Be sure to change the P**eripheral Device Type** to suit your operating system after the in-band host links have been properly connected.
2. Operating Infortrend RAID systems does not require OS driver. If you select **All Undefined LUNs** in the **LUN Applicability** menu, every mapped volume will cause a message prompt in the OS asking for the support driver.

Chapter 4

Configuration Client Options

This chapter describes the Configuration Client options. There are a number of different items that users can configure. These include the Root Agent and RAID Agents relationship and the configuration options concerning event notification. The following sections are covered in this chapter:

- **The Configuration Client Utility – Section 4.1, page 4-2**
  - **4.1.1 Start the Configuration Client**
  - **4.1.2 Setting Up a Root Agent**
- **Configuration Client – Section 4.2, page 4-7**
  - **4.2.1 Command Menu**
  - **4.2.2 Tool Bar Buttons**
  - **4.2.3 Connection View Window**
  - **4.2.4 Module Configuration Window**
- **Root Agent Configuration – Section 4.3, page 4-10**
  - **4.3.1 Root Agent Settings**
  - **4.2.2 Tool Bar Buttons**
  - **4.3.3 Root Agent Log Settings**
  - **4.3.4 Create Plug-ins**
- **Event Notification Settings – Section 4.4, page 4-13**
  - **4.4.1 Configuration Client Notification Methods**
  - **4.4.2 Event Severity Levels**
  - **4.4.3 Enabling Notification Functions**

- **4.4.4 SNMP Traps Settings**
- **4.4.5 Email Settings**
- **4.4.6 LAN Broadcast Settings**
- **4.4.7 Fax Settings**
- **4.4.8 MSN Settings**
- **4.4.9 SMS Settings**

♦ **Auto Discovery – Section 4.5, page 4-31**

♦ **Event Severity Levels – Section 4.6, page 4-33**

- **4.6.1 Level 1 Severity Events (Examples)**
- **4.6.2 Level 2 Severity Events (Examples)**
- **4.6.3 Level 3 Severity Events (example)**

♦ **Event Log Display – Section 4.7, page 4-35**

4.1 The Configuration Client Utility

4.1.1 Start the Configuration Client Program

If the Centralized Management option was selected during the installation process outlined in ***Chapter 2***, the Root Agent driver, associated agents, and Configuration Client utilities will be installed onto your computer. Centralized management in a multi-RAID environment is achieved through the Configuration Client utility.

To access the Configuration Client interface, please do the following:

Step 1. Open the directory in which the SANWatch management software was installed. The directory was selected during the installation process and the default access route was named "***Infortrend Inc***."

Step 2. If you are using a Windows operating environment, you may start the Configuration Client by double-clicking on

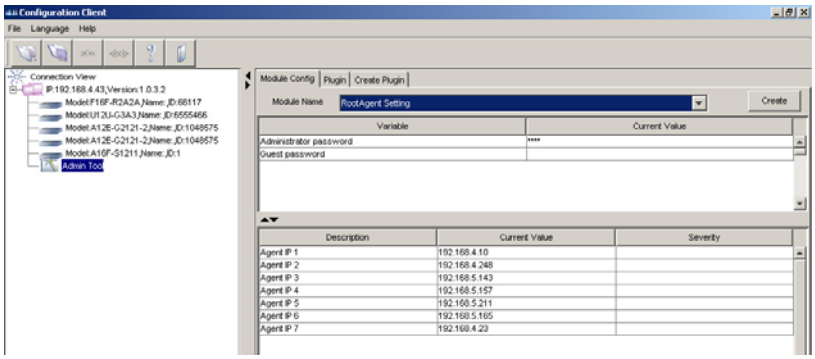
the ***Configuration Client*** shortcut on your Windows Desktop.

Otherwise, select ***Start*** on the bottom left of your screen, select the ***Programs*** menu, and then select ***Infortrend Inc.*** Under the ***Infortrend Inc*** directory, select the ***Configuration Client*** option.

Figure 4-1: Configuration Client Shortcut on Windows Startup Menu

Step 3. Click on ***Configuration Client*** to activate the Configuration Client window**.** The Configuration Client program allows you to configure the following items:

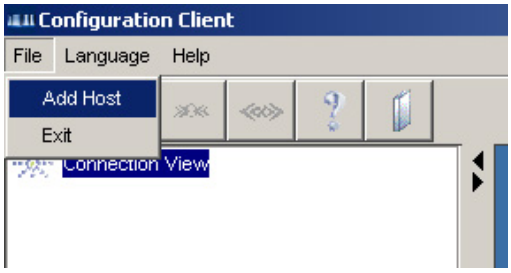
- Root Agent (administrative settings)
- Auto Discovery
- Notification configuration options

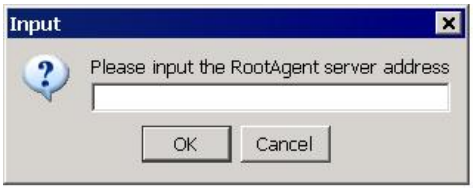


4.1.2 Setting Up a Root Agent

Step 1. Launch the Configuration Client program. See ***Section 4.1.1***.

Step 2. From the Command menu, select **File->Add Host**, or right-click on ***Connection View*** to bring up the **Add Host** Dialog Box, and enter a **Root Agent IP** here.



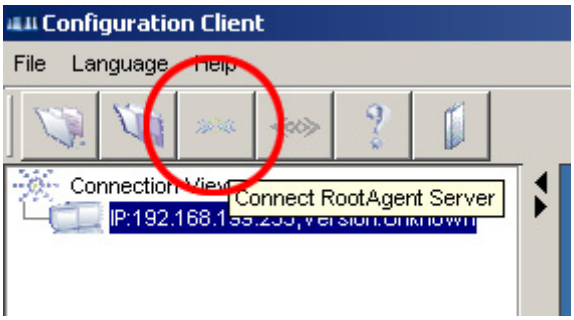


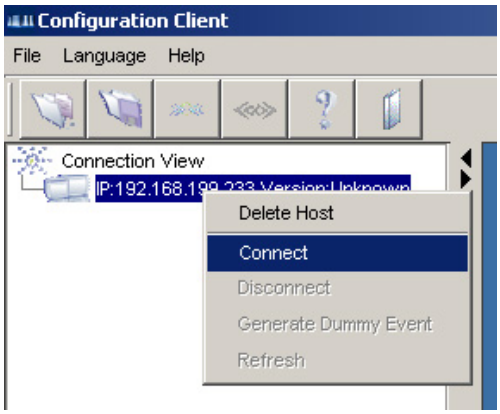
NOTE:

The Root Agent IP is usually the computer IP where the Configuration Client is installed using SANWatch's **Custom** mode -> **Central Management** installation option.

Step 3. The connected IP displays on the left of the **Connection View** window. Select the IP and click the ***Connect Root***

Agent Server icon or right-click on the displayed IP to display the ***Connect*** commands.

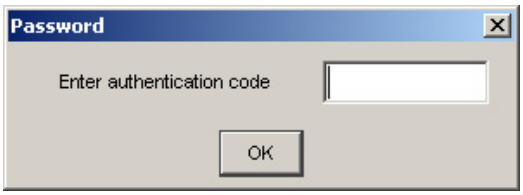




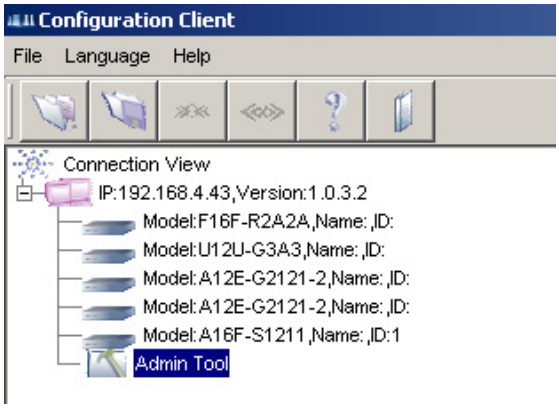
Step 4. The **Configure user** dialog box appears. Select to log in either as an Administrator or Guest. An administrator has the authority to change any configuration client settings, unlike a guest is allowed to view the settings only. (See *Error! Reference source not found.*)

Step 5. When login as an administrator, enter "***root***" as the authentication code in the **Password** dialog box at the first time login, and then click ***OK***. (See *Error! Reference source not found.*) The authentication code can be changed later in the utility. Only an administrator who has the password can access the notification settings.

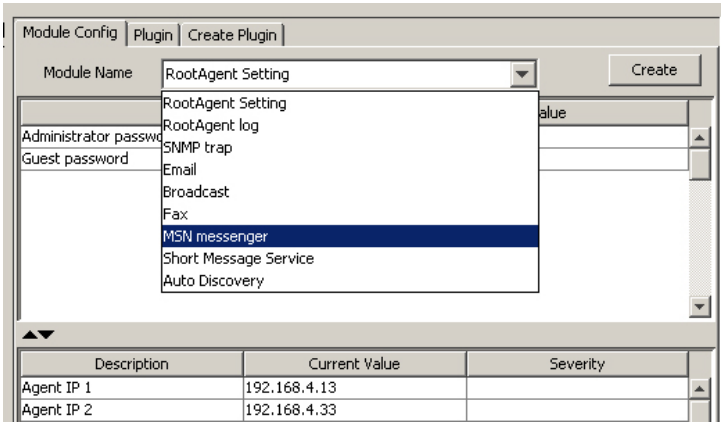
Step 6. Password is not required when login as a guest. Click ***OK*** to login without entering any password.



Step 7. Double-click the **Admin Tool** item on the **Connection View** window that appears when a Root Agent is successfully connected.

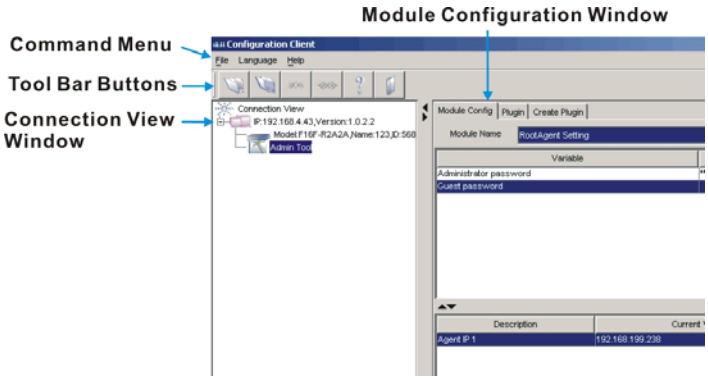


Step 8. The **Module Configuration** window will display on the right of the **Configuration Client** configuration screen. You may now start configuring event receivers under each notification method window. Click on the **Module Name** pull-down list to display all the configuration options.



4.2 Configuration Client User Interface

The Configuration Client user interface contains four (4) major elements: Tool Bar Buttons, Connection View Window, and Module Configuration Window.



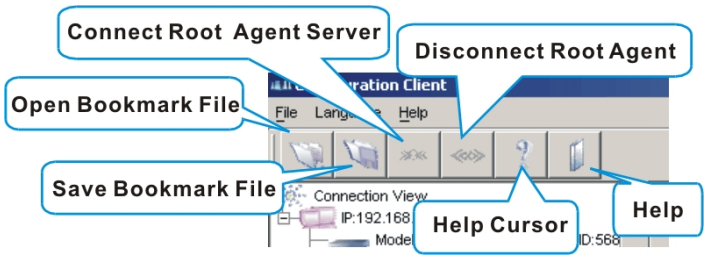
4.2.1 Command Menu

- The **File** commands include **Add Host** and **Exit**. The **Add Host** command connects you to a Root Agent host. A Root Agent host is one that is chosen as a management center to manage multiple RAID agents, which are, in turn, used to access different arrays. By connecting to one or multiple Root Agents, all its subsidiary RAIDs are then managed by the management center. The **Exit** command will let you exit the **Configuration Client** user interface and close the program.

- The **Language** command allows you to select the language display on the **Configuration Client User Interface**. The current selections include English, Deutsch, Spanish and Japanese.

- The **Help** command provides information about the current software version. The **Help** explains how to use the Configuration Client and can be accessed in SANWatch's main Help program.

4.2.2 Tool Bar Buttons



The tool bar has six (6) buttons, described from left to right as follows:

- **Open Bookmark File***:* In the environment where multiple arrays need to be monitored at the same time, this button brings out the previously saved profile of the access to multiple arrays (via Root Agent and RAID Agent IPs).

- **Save Bookmark File***:* This button allows you to save the current connection profile (as shown in the Navigation panel) as a file to your system drive. A file path dialog box displays when selected.

- **Connect Root Agent Server***:* This button allows you to connect to a Root Agent server to begin monitoring, for example, in situations when it has been manually disconnected.

NOTE:

The Root Agent IP is the IP of the computer where you installed your Configuration Client utility.

- **Disconnect Root Agent***:* This button allows you to disconnect from a Root Agent server.

- **Help Cursor***:* Click the ***Help Cursor*** button and then click on the area where you have question. A **Help** window will appear to explain the functionality.

- **Help***:* Click on the ***Help*** button to browse the Online Help in SANWatch management software's main Help program.

4.2.3 Connection View Window

The **Connection View** window displays the current connections with different RAID Agent servers. Each Root Agent server IP has an Administration Tool. This window has a command menu that can be

triggered by *right-clicking* a Root Agent icon. Right-click on the Root Agent server to show a selection menu. (See ***Figure 4-2***)

These commands on the selection menu allow you to remove a Root Agent entry, to connect, disconnect, or refresh the current connectivity status. The **Connection View** window automatically updates when an array is turned on or off, and automatically prompts you for a status change, e.g., a managed array once disconnected is now connected.

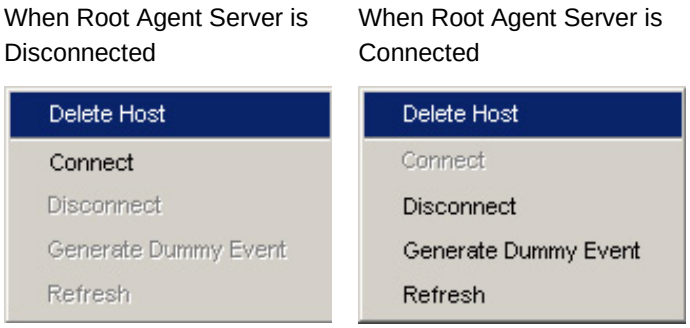


Figure 4-2: Connection: The Right-click Menus

Delete Host: Delete the Root Agent Server by selecting this command.

Connect: Select this command to connect your computer to the Root Agent Server.

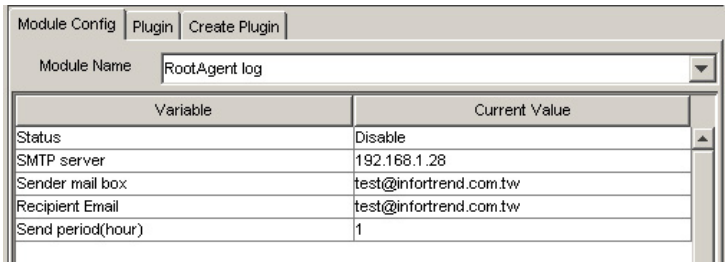
Disconnect: To disconnect the Root Agent Server from your computer, select this command.

Generate Dummy Event: You can also generate simulated events to test the notification functions once you have configured any or all of the notification methods.

Refresh: Refresh the connection between your computer and the Root Agent Server.

4.2.4 Module Configuration Window

The ***Module Config*** panel contains pull-down menus that allow access to create or modify various notification methods. The panel also allows you to setup an administrator's identity and lets an administrator be constantly aware of all arrays' status through notification emails.



The **Module Config** panel provides access to ten (10) configurable items, and each item contains two or more setup options. Seven (7) of them belong to the notification methods (ways to notify a user if event faults occur) settings.

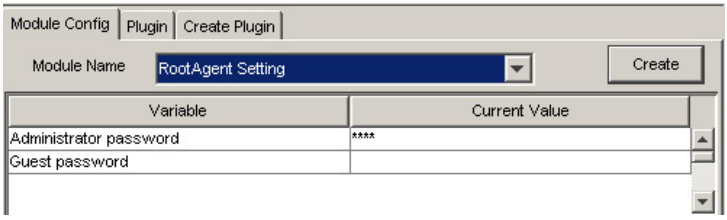
Double-clicking the **Current Value** field can modify all configuration options.

4.3 Root Agent Configuration

To configure the Root agent settings, select the ***Module Config*** menu on the right of the Configuration Client User Interface as shown below. Select the pull-down menu named ***Root Agent Setting*** from the ***Module Name*** section.

4.3.1 Root Agent Settings

The ***Root Agent Setting*** option is shown below:



- **Administrator Password**: This allows you to set an administrator's password. This is the port number the SANWatch centralized manager station will use to communicate with the Root Agent. The default for Administrator is "**root**." There is no default password for login as Guest.

NOTE:

This password is independent from the password set for the

"Configuration" login to start the SANWatch management program.

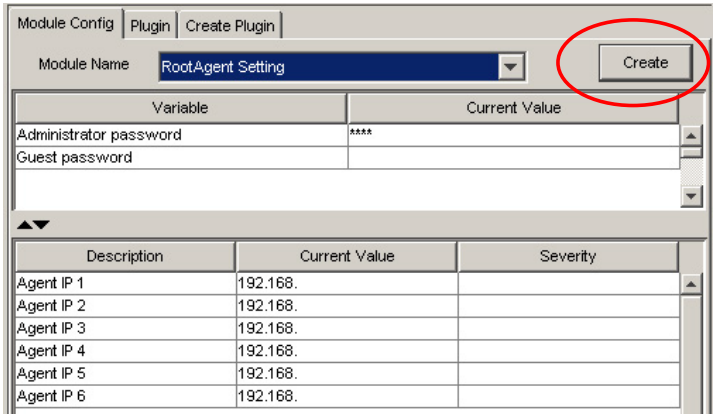
- **Guest Password:** This is selected to enable a user logging in as "Guest" to view the status of RAID arrays currently being managed by the Configuration Client utility.

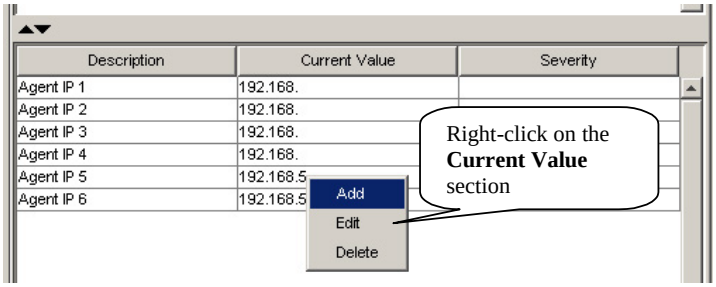
4.3.2 Adding RAID Agents IPs (Associating Root Agent with Multiple RAID Arrays)

RAID Agents are the sub-modules of SANWatch or the Configuration Client utility used to communicate with a RAID subsystem. Multiple RAID Agents can be associated with a Root Agent. A Root Agent then summarizes and presents these RAID Agents to the Configuration Client so that system administrators can be notified of system alerts if faulty conditions are detected within these RAID arrays.

Step 1. RAID Agents currently being managed by a Root Agent are listed in the lower right corner of the Configuration Client screen.

Step 2. To add or delete RAID Agents, click the ***Create*** button next to the **Root Agent** pull-down list to open an ***Add Monitor Controller*** window. (See *Error! Reference source not found.*) The same command can also be activated by right-clicking on the agent list under ***Current Value*** section.





Step 3. Enter the IP address of the array you wish the Root Agent to manage. Click ***OK*** to complete the process. An example is shown below.

4.3.3 Root Agent Log Settings

Following are the methods used to keep an administrator constantly notified of the status of managed arrays. As shown in the following screen captures**,** when properly configured, the Root Agent Log allows an administrator to receive event logs for all managed arrays for every preset time period.

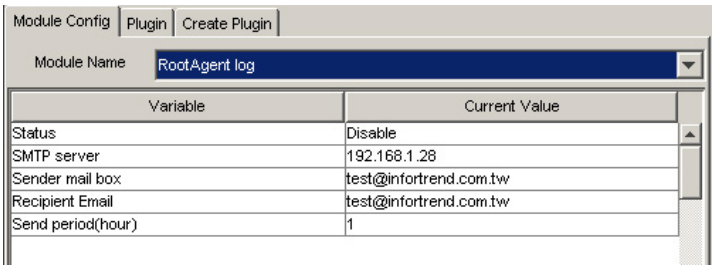
To configure the ***Root Agent Log*** settings:

Step 1. Enable the function by double-clicking the Current Value field in the Status field.

Step 2. Set an SMTP server address in the **SMTP server** field so that event log emails can be sent to the administrator.

Step 3. Set a valid mail address in the **Sender mailbox** field and an administrator's email address in the **Recipient Email** field.

Step 4. The **Send period (hour)** determines how often an administrator receives event log notifications.



4.3.4 Create Plug-ins with Event Notification

Step 1. Before you begin

- The **Plug-in** sub-function allows you to add a specific feature or service to SANWatch's notification methods.

- The add-ins can be used to process the events received from Configuration Client utility and extend its functionality.

  Prepare your execution file, and place it under the **plug-in** sub-folder under the directory where you installed the SANWatch program. If the default installation path has not been altered, the plug-in folder should be similar to the following:

  Program Files -> Infortrend Inc -> RAID GUI Tools -> bin -> plug-in.

  Place the execution file that will be implemented as a plug-in in this folder.

The plug-in capability provides advanced users the flexibility to customize and present the event messages received from the Configuration Client utility.

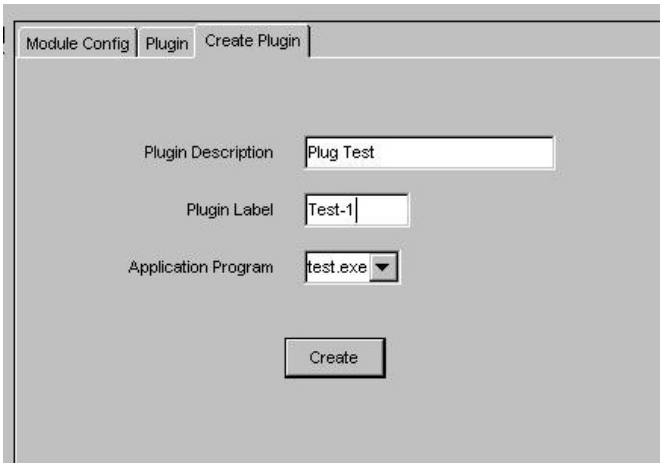
Step 2. The Configuration Process

Step 1. Click the Create **Plug-in** tab.

Step 2. Make sure you have placed the execution file in the **plug-in** folder as described earlier.

Step 3. Enter the appropriate data in the Plug-in Description and Plug-in Label fields, and then select an execution file from the ***Application Program*** field (if there is more than one).

Step 4. Click ***Create*** to complete the process.

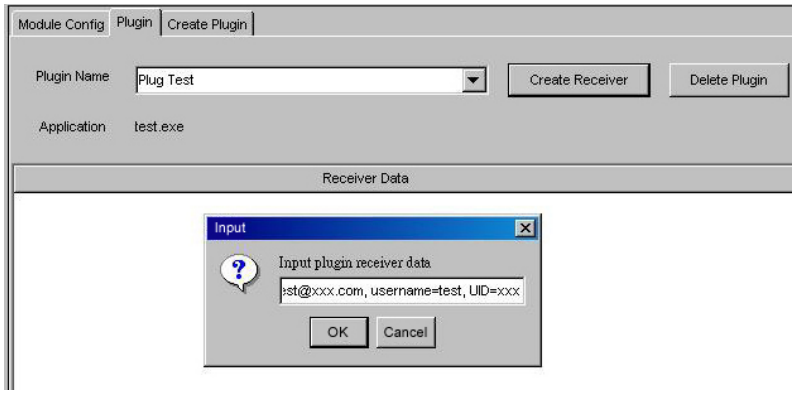


Step 5. Select the ***Plug-in*** tab from the panel. Click ***Create Receiver*** to display an input field dialog box.

Step 6. Enter the configuration string to be read when the application program starts. A configuration argument may look like this:

"\plugin\userprogram.exe uid=xx model=xxx-xxx ip=xxx.xxx.xxx.xxx ctrlrName=N/A severity=1 evtStr="Evt String" recv="customized string"

An added profile is listed in the **Receiver Data** field.



4.4 Event Notification Settings

4.4.1 Configuration Client Notification Methods

Configuration Client provides the following methods for sending notifications: **SNMP traps**, **email**, **LAN broadcast**, **fax**, **SMS**, and **MSN Messenger**. Some notification methods, such as the connection to a fax machine, require Windows MAPI support on the servers used as the Configuration Client platform.

To configure the Event Notification (previous *NPC*) settings, select ***Module Config*** from the right-hand side of GUI screen. Scroll down the pull-down menus to create or modify various notification methods.

There are seven notification methods listed in the pull-down menus. Along with seven different means of informing RAID managers that an event has occurred (fax, broadcast, email, SNMP traps, SMS, and MSN messenger), the severity level of events to be sent via these notification methods can also be configured.

4.4.2 Event Severity Levels

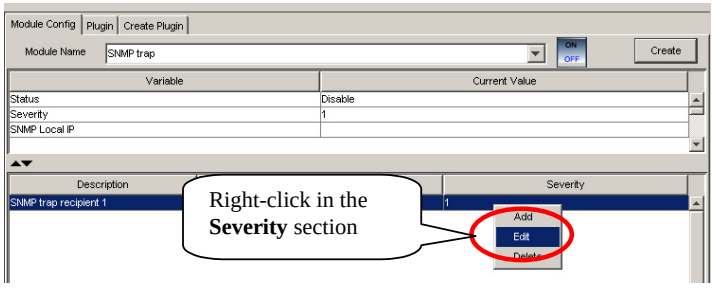
You may select a severity level for every notification method using the Event Severity Level setting. Each level determines events of what severity level(s) are to be sent to a receiver. See ***Table 4-1*** for severity level descriptions.

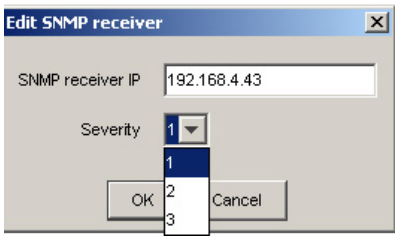
Level	Description
1	All severity levels

2	Two levels: Warning and Alert
3	Only the most serious events: Alert messages

Table 4-1: Levels of Notification Severity

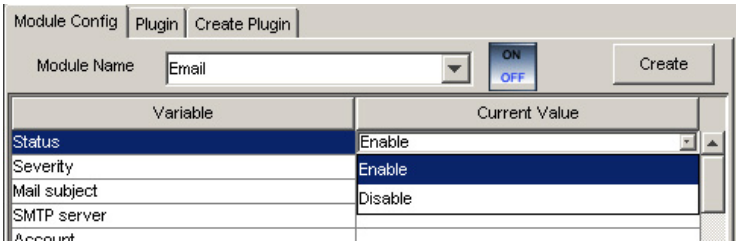
The event security level can be set during notification function setting. If you wish to modify the security levels for any notification setting, right-click on the ***Severity*** section in the lower level of **Configuration** screen. Select the **Edit** common to view the **Edit** dialog box. Select the desired severity level in the **Severity** pull-down menu. Once the severity level is selected, click ***OK*** to exit the dialog box.





4.4.3 Enabling Notification Functions

When all notification settings have been properly configured, remember to enable each notification method by double-clicking the ***Current Value*** field in **Status** row. Set **Status** to ***Enable*** if you want the module to be activated every time the Root Agent is loaded.



You can also turn on and off each notification method by double-clicking on the switch button located on the upper left of the user interface. The Root Agent runs as an application and is automatically loaded when the

server is powered on. Restart the Configuration Client for the changes to take effect.

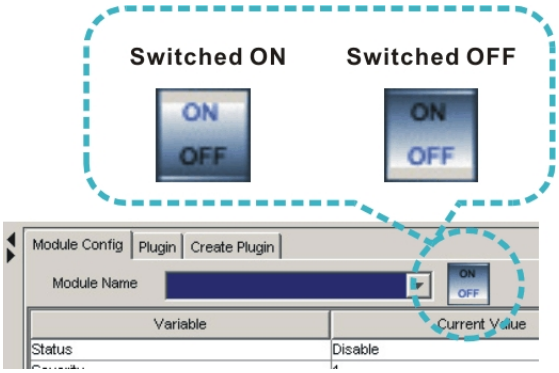


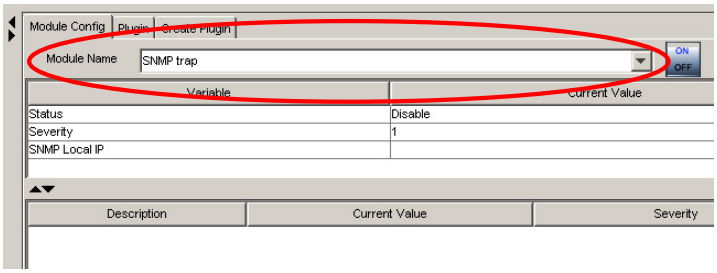
Figure 4-3: Enabling a Notification Method by the Switch Button

4.4.4 SNMP Traps Settings

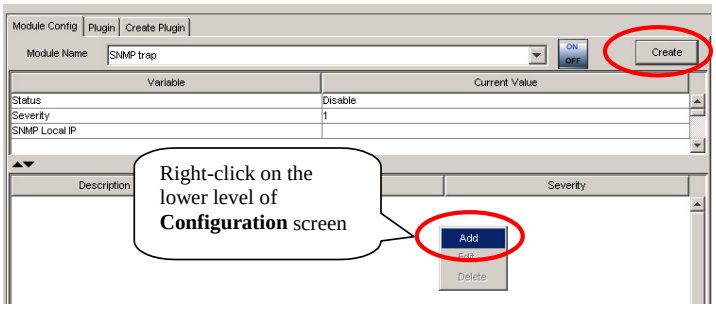
Receiver Side

To set a client listening to SNMP traps:

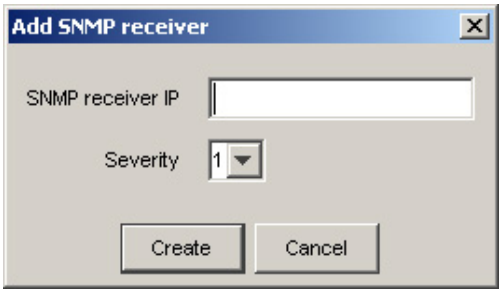
Step 1. Open the ***Module Config*** page. Use the ***Module Name*** pull-down menu to select ***SNMP trap***.



Step 2. To create a new SNMP trap, click the ***Create*** button on the top right screen or right-click on the lower half of the configuration screen; the **Add SNMP Receiver** dialog box will appear.



Step 3. Enter the IP addresses of the SNMP agents that will be listening for trap notification in the **Add SNMP Receiver** dialog box



Step 4. Select the severity level of events that will be sent to the SNMP agent. Refer to ***Section 4.4.2.***

Step 5. Repeat this process to add more SNMP agents.

Sender Side

From the Module Config window:

Step 1. Find the SNMP settings from the pull-down list.

Step 2. Click on the ***On/Off*** switch beside the pull-down button to enable SNMP traps notification.

Switched ON Switched OFF

Step 3. Double-click on the Current Value field of the Status row to enable SNMP traps notification.

Step 4. Select the severity level of events to be sent to the receiver station.

Step 5. Provide a valid out port IP that will be used for delivering SNMP traps. Usually the default IP detected by the Root Agent will be sufficient. If you have more than one Ethernet port, double-click to configure it.

4.4.5 Email Settings

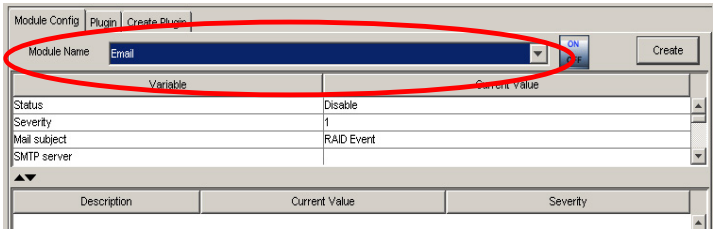
Receiver Side

NOTE:

SASL authentication is supported with this revision.

To set an email address to receive notification emails:

Step 1. Open the **Module Configuration** page. Use the **Module Name** pull-down menu to select **Email**.



Step 2. To create a new email notification, click the ***Create*** button on the upper right corner of the screen or right-click on the lower half of the configuration screen to display the **Add Email Recipient** dialog box.

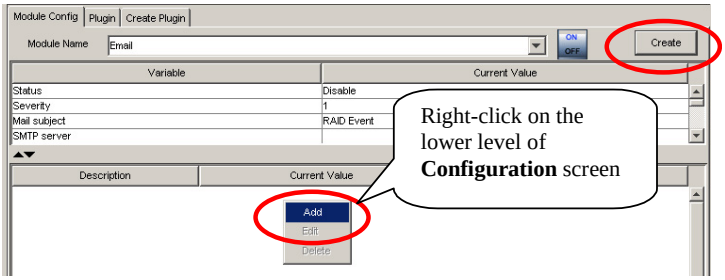
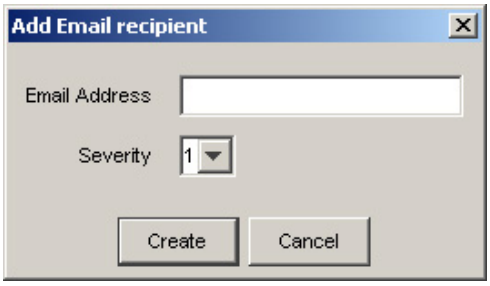


Figure 4-4: Adding Email Notification

Step 3. An **Add Email Recipient** dialog box appears. Enter a receiver's email address.



Step 4. Select the severity level of the events to be sent to the receiver's email.

Step 5. Repeat this process to add more receiver addresses.

Sender Side

From the Module Config window:

Step 1. Find the email settings from the ***Module Name*** pull-down list.

Step 2. Click the On/Off switch beside the pull-down list button to enable Email notification.

Switched ON Switched OFF

Step 3. Double-click on the **Current Value** field of the Status row to enable email notification.

Step 4. Select the severity level of events to be sent to the receiver station.

Step 5. Enter the mail subject by double-clicking the **Current Value** field and entering a mail subject.

Step 6. Set your SMTP mail server through which the notification emails will be sent.

Step 7. Enter the Account name and Password if your mail server requires these values. SASL is the currently supported mechanism.

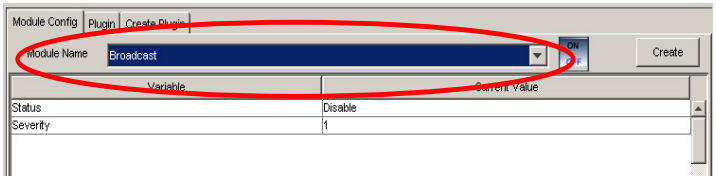
Step 8. Provide a valid email address as your sender's address.

4.4.6 LAN Broadcast Settings

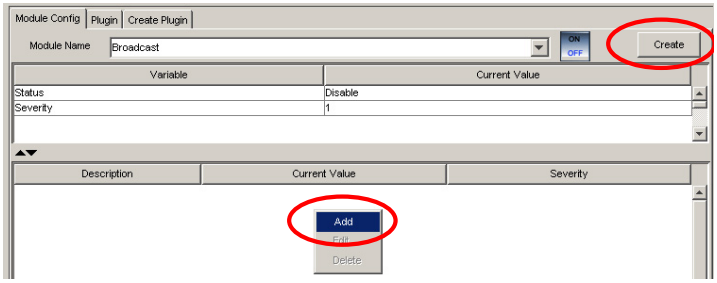
Receiver Side

To set a computer to receive broadcast messages:

Step 1. Open the **Module Configuration** page. Use the **Module Name** pull-down menu to select **Broadcast**.



Step 2. To create a new LAN broadcast notification, click the ***Create*** button on the upper right corner of the screen or right-click on the lower half of the configuration screen to display the **Add Broadcast Recipient** dialog box.



Step 3. An **Add Broadcast Receiver** dialog box appears. Simply enter the IP addresses of a station configured on a network.

Step 4. Select the severity level of the events to be sent to the receiver station.

Step 5. Repeat this process to add more receivers.

NOTE:

NETBUES and TCP/IP should be active services on your Centralized Management station for message broadcasting.

Sender Side

From the Module Config window:

Step 1. Find the Broadcast settings from the pull-down list.

Step 2. Click on the On/Off switch beside the pull-down button to enable LAN broadcast notification.

Switched ON Switched OFF

Step 3. Double-click on the Current Value field of the Status row to enable LAN broadcast. Set Status to Enable if you want the module to be activated every time the Root Agent is started. Note that the On/Off switch should also be in the ON position before you turn off the server or close the utility. Otherwise, you will have to manually enable the function whenever you reboot the server.

Step 4. Select the severity level of events to be sent to the receiver station.

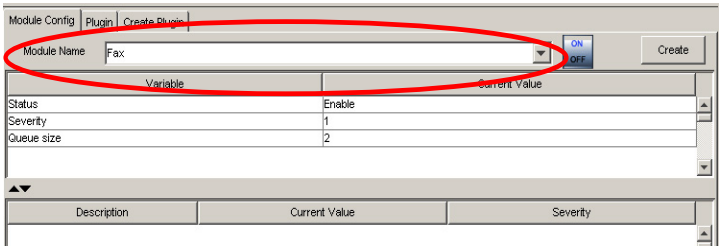
4.4.7 Fax Settings

In order to use fax notification, a fax modem is required and its parameters must be properly set on the main management station. For NT servers, Widows MAPI services, modem, and fax must be ready and running for the notification methods to work.

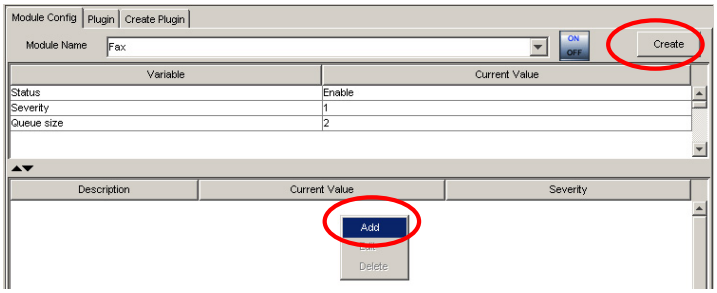
Receiver Side

To set a fax machine to receive event messages:

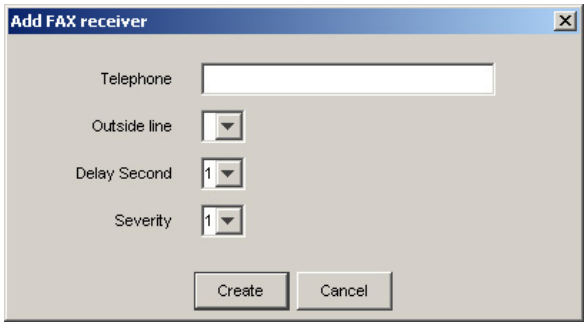
Step 1. Open the **Module Configuration** page. Use the **Module Name** pull-down menu to select **Fax**.



Step 2. To create a new Fax notification, click ***Create*** on the upper right corner of the screen or right-click on the lower half of the configuration screen to display the **Add Fax Recipient** dialog box.



Step 3. An **Add Fax Receiver** dialog box prompts. Enter the phone number of the fax machine that will receive event notifications.



Step 4. Enter the Outside line dial-out number if there is any.

Step 5. Enter the Delay Second number.

Step 6. Enter the level of **Severity** of the events to be sent via fax.

Step 7. Repeat this process to add more receivers.

NOTE:

The physical connection and fax service with Windows MAPI should be ready before configuring this function.

Sender Side

From the Module Config window:

Step 1. Find the Fax settings from the pull-down list.

Step 2. Click on the On/Off switch beside the pull-down button to enable Fax notification.

Switched ON Switched OFF

Step 3. Double-click on the Current Value field of the Status row to enable fax notification. Set Status to Enable if you want the module to be activated every time the Root Agent is started. Note that the On/Off switch should also be in the On position before you turn off the server or close the utility. Otherwise, you will have to manually enable the function whenever you reboot the server.

Step 4. Select the severity level of events to be sent to the receiver station.

Step 5. The Fax device row shows the fax machine(s) currently available. Check for appropriate setup in the Windows control panel.

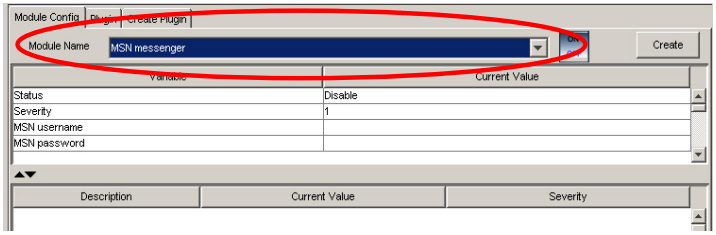
Step 6. Queue size determines how many events will be accumulated and then sent via a single fax transmission.

4.4.8 MSN Settings

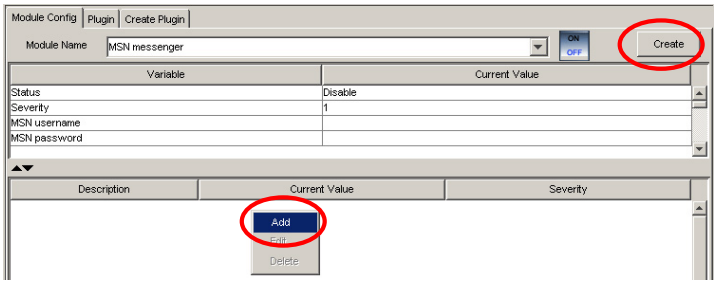
Receiver Side

To set an MSN messenger address to receive notification messages:

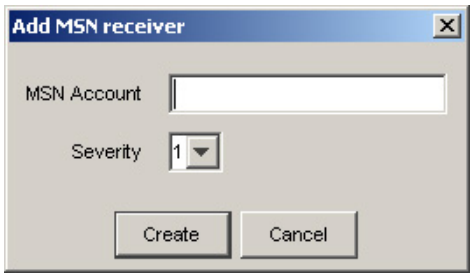
Step 1. Open the **Module Configuration** page. Use the **Module Name** pull-down menu to select MSN.



Step 2. To create an MSN notification, click ***Create*** on the top right of the screen or right-click on the lower half of the configuration screen to display the **Add MSN Recipient** dialog box.



Step 3. Enter the MSN account of the contact receiving event messages.



Step 4. Select the severity level of events to be sent to the receiver.

Step 5. Repeat this process to add more receivers.

Sender Side

From the **Module Config** window:

Step 1. Find the MSN settings from the pull-down list.

Step 2. Click on the On/Off switch beside the pull-down button to enable MSN notification.

Switched ON

Switched OFF

Step 3. Double-click on the **Current Value** field of the Status row to enable MSN notification. Set Status to Enable if you want the module to be activated every time the Root Agent is started. Note that the On/Off switch should also be in the ON position before you turn off the server or close the utility. Otherwise, you will have to manually enable the function whenever you reboot your server.

Step 4. Select the severity level of events to be sent to the receiver station.

Step 5. Provide a valid MSN contact by entering the user name.

Step 6. Provide the associated password.

4.4.9 SMS Settings

SMS is a short for "Short Message Service." Using this notification method requires a GSM modem. SANWatch currently supports two GSM modem models:

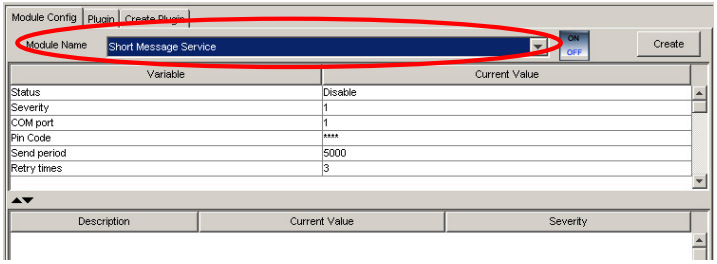
- Siemens TC35
- WAVECOM Fast Rack M1206

Please contact Infortrend for the complete list of compatible GSM modems.

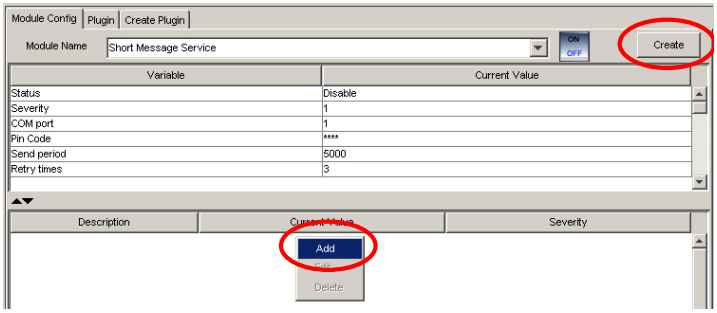
Receiver Side

To set a cell phone to receive notification messages:

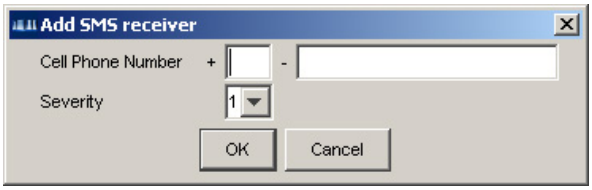
Step 1. Open the **Module Configuration** page. Use the **Module Name** pull-down menu to select SMS Message Service.



Step 2. To create a new SMS notification, click the ***Create*** button on the upper right of the screen or right-click on the lower half of the configuration screen to display the **Add SMS Recipient** dialog box.



Step 3. Enter the **Cell Phone Number** of the contact who will receive event messages.



Step 4. Select the severity level of events to be sent to the receiver.

Step 5. Repeat this process to add more receivers.

Sender Side

From the Module Config window:

Step 1. Find the SMS settings from the pull-down list.

Step 2. Click on the On/Off switch beside the pull-down button to enable SMS notification.

Switched ON

Switched OFF

Step 3. Set Status to Enable if you want the module to be activated every time the Configuration Client is started. Note that the On/Off switch should also be in the On position before you turn off the server or close the

utility. Otherwise, you will have to manually enable the function whenever you reboot the server.

Step 4. Select the severity level of the events to be sent to the receiver station.

Step 5. Select the COM port where you connect your GSM modem.

Step 6. Enter the four-digit identification Pin Code required by the modem.

Step 7. Provide a Send Period in milliseconds for time intervals between messages to be sent.

Step 8. Provide a retry time value.

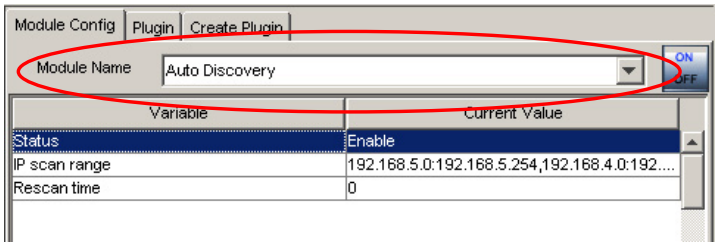
4.5 Auto Discovery

The innovative **Auto Discovery** feature provides quick, instant agent search function. If this option is enabled, the system will automatically search for the available agents and add it into agent list without manually key-in each agent IP address.

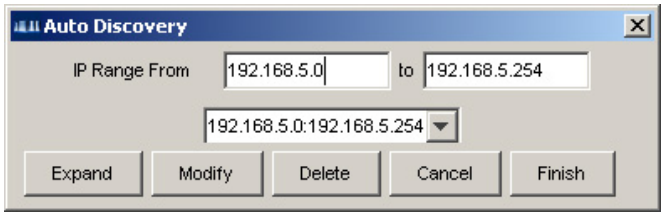
The **Auto Discovery** option also enables root agents to be discovered on the **Central Management** utility.

To setup the Auto Discovery option, please follow the steps below:

Step 1. Open the **Module Configuration** page. Use the **Module Name** pull-down menu to select Auto Discovery option.



Step 2. Double-click on the current value under **IP scan range** row to open the Auto Discovery dialog box.



Step 3. Enter a set of IP range that you want the system to detect in the IP range dialog box.

NOTE:

You may modify an existing IP range by clicking the Modify button or delete an existing IP range by clicking the Delete button. Click on the Cancel button to cancel any action you made in the Auto Discovery dialog box and return to the Auto Discovery main screen.

Step 4. Click the **Expand** button to add the new IP range into a preset list.

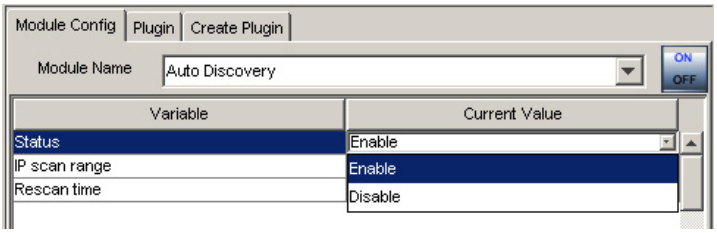
Step 5. Click the **Finish** button to close this dialog box and return to the Auto Discovery option main screen.

Step 6. Double-click on the current value on **Rescan time** row to modify a time frame in minute that you like the system to scan the network.

NOTE:

The default rescan time is set to **0** minute that indicates the system will scan the network only when Configuration Client is started. The Auto Discovery option will not be repeated after the first scan.

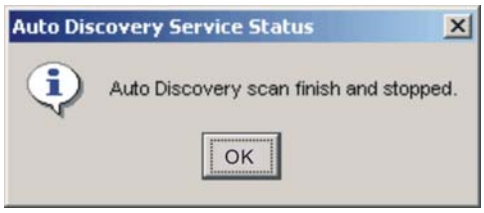
Step 7. You may turn on and off this option by double click on current value on the **Status** row or click on the On/Off switch beside the pull-down button to enable the option.



NOTE:

If you already have the Auto Discovery option turned on, be sure to turn off and then turn on the option for any adjustments that you newly made to take effect.

Once the Auto Discovery option is successfully configured, the system will detect the IP range that you designated, and automatically add the search results into the agent list. An Auto Discovery Notice window will prompt, you may click ***OK*** button to close the window and start using Configuration Client and SANWatch Manager.



If you open the Root Agent setting option on the module configuration window, an available agent list will be shown in the lower section of the Configuration Client user interface. (See ***Figure 4-5***)

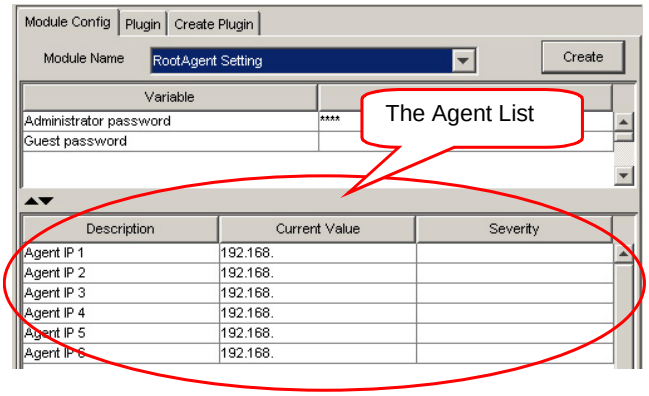


Figure 4-5: The Root Agent List

If you like to start using the SANWatch manager, please refer to ***Section 5.2***. An ***Agent List window*** will automatically display the controllers that were detected by the Auto Discovery option.

4.6 Event Severity Levels

SANWatch classifies disk array events into three severity levels. Level 1 includes non-critical information events such as initialization of the controller and initiation of the rebuilding process. Level 2 severity includes events which require the issuance of a warning message. Level 3 severity is the most serious level, and includes events that need immediate attention. The following provides example events for each level:

4.6.1 Level 1 Severity Events (Examples)

- Controller Initialization Complete
- Rebuild Initiated
- Rebuild Complete

- Rebuild Failed
- Logical Drive Initialization Started
- Logical Drive Initialization Complete
- Logical Drive Initialization Failed

4.6.2 Level 2 Severity Events (Examples)

- SCSI Target Select Timeout
- SCSI Target Phase/Signal Error
- SCSI Target Unexpected Disconnect
- SCSI Target Negotiation Error
- SCSI Target Timed Out
- SCSI Target Parity Error
- SCSI Bus Reset Issued
- SCSI Target Not Ready Error
- SCSI Target Media Error
- SCSI Target Hardware Error
- SCSI Target Unit Attention
- SCSI Target Unexpected Sense Date
- SCSI Target Block Reassignment Failure
- SCSI Target Unexpected Data Over/Underrun
- Drive SCSI Unrecognized Event

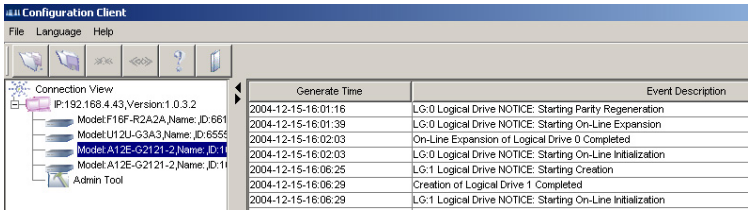
4.6.3 Level 3 Severity Events (example)

- Drive Failure
- Enclosure Power Supply Failure
- Cooling Fan Module Failure
- RAID Controller Unit Failure

4.7 Event Log Display

Once RAID Agent IPs are associated with a Root Agent, their icons and names display on the Connection View panel.

To refer to the events that have happened since the Configuration Client started, single-click on a connected RAID. Note that the Configuration Client station should be one that is always on so that important messages will not be ignored.



The event log window displays on the right-hand side of the SANWatch screen.

NOTE:

The utility does not display events that happened before the utility is started.

This page is intentionally left blank.

Chapter 5

SANWatch Icons

This chapter introduces icons used in the main configuration access categories:

- **Navigation Tree Icons – Section 5.1**
- **Information Icons – Section 5.2**
- **Maintenance Icons – Section 5.3**
- **Configuration Icons – Section 5.4**
- **Event Log Icons – Section 5.5**

5.1 Navigation Tree Icons

	Connected RAID Array

	Information	
		Enclosure View
		Tasks Under Process
		Logical Drive Information
		Logical Volume Information
		Fibre Channel Status
		System Information
		Statistics

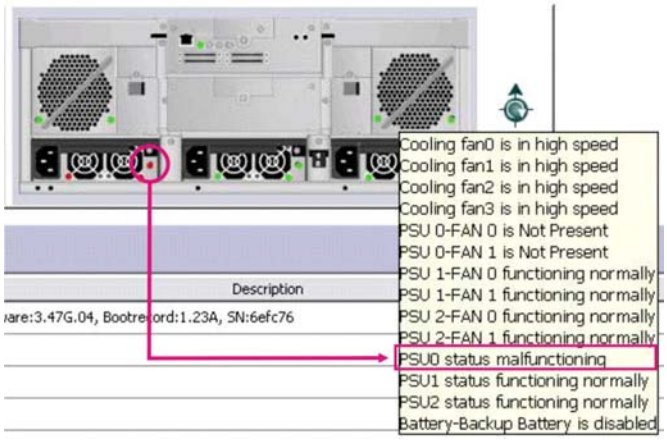
	Maintenance	
		Logical Drive
		Physical Drive
		Task Scheduler

	Configuration	
		Quick Installation
		Installation Wizard
		Create Logical Drive
		Existing Logical Drives
		Create Logical Volume
		Existing Logical Volumes
		Host Channel
		Host LUN Mapping
		Configuration Parameters

	Data Service	
		Snapshot Information
		Configure Snapshot
		Maintain Snapshot

	Agent	
		Snapshot Agent
		Snapshot Schedule

5.2 Array Information Icons

Enclosure View	
	Drive in good condition
	Drive missing or failed
	Global Spare
	Any drive icon showing a color other than black represents a member of a logical drive or a dedicated spare. Black is the default color of a new or used drive. A used drive is a drive that had been used as a member of a logical drive.
	An empty tray; disk drive not installed
	This graphic represents a rotation button. Each mouse-click on it turns the enclosure graphic 90 degrees clockwise.
	

SANWatch recognizes each subsystem by its board serial number, and displays an exact replica of it in the panel view.

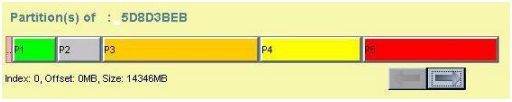
LEDs shown on the enclosure view correspond to the real LEDs on the subsystem.

If an LED corresponding to a failed component is lit red as shown above, move your mouse cursor to the enclosure panel. Let the cursor stay on the graphic for one second and an enclosure status summary will be displayed.

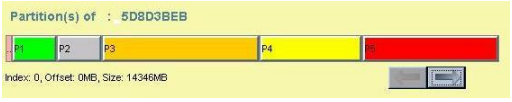
Tasks Under Process

	Type of tasks being processed by the subsystem. The Task status window displays icons representing specific configurations.
	Progress indicator

Logical Drive Information

	A logical drive
	A partitioned logical drive volume is represented as a color bar that can be split into many segments. Each color segment indicates a partition of a configured array.

Logical Volume Information

	A logical volume
	A partitioned logical volume is represented as a color bar that can be split into many segments. Each color segment indicates a partition of a configured volume.
	A member of a logical volume, representing a logical drive. Different logical drives are presented using icons of different colors.

Fibre Channel Status	
	A Fibre host channel

System Information	
	A battery module
	A RAID controller unit
	A current sensor
	A cooling module
	An enclosure device connected through an I^2C bus
	A power supply
	An enclosure device connected through SAF-TE (SCSI bus)
	An enclosure device connected through SES (Fibre link)
	A drive tray slot
	A temperature sensor
	An UPS device
	A voltage sensor

5.3 Maintenance Icons

Maintenance
This category uses the same icons as in the Logical Drive Information window. See ***Logical Drive Information*** section.

5.4 Configuration Icons

Create Logical Drives

This window uses the same icons as in the Logical Drive Information window. See ***Logical Drive Information*** section.

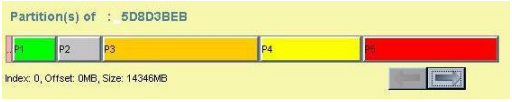
Existing Logical Drives

	A configured array (logical drive)

Create Logical Volume

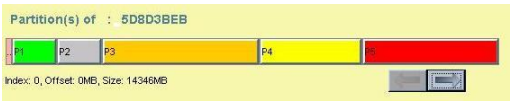
	A member of a logical volume, representing a logical drive. Different logical drives are presented using icons of different colors.

Existing Logical Volumes

	A logical volume
	A partitioned logical volume is represented as a color bar that can be split into many segments. Each color segment indicates a partition of a configured array.
	A member of a logical volume, representing a logical drive. Different logical drives are presented using icons of different colors.
	A logical volume

Host Channel

	A host channel

Host LUN Mapping	
	A logical drive. Different logical drives are presented using icons of different colors.
	A logical volume
	A partitioned array volume is represented as a color bar that can be split into many segments. Each color segment indicates a partition of a configured array.

Configuration Parameters
No icons are used in the window.

5.5 Event Log Icons

Event Messages	
Severity Levels	
	An informational message: Command-processed message sent from the firmware
	A warning message: System faults or configuration mistakes
	An alert message: Errors that need immediate attention
Event Type	
Type of messages detected by the subsystem. The event view panel displays icons representing specific categories using the same icons as those used in the System Information window.	

This page is intentionally left blank.

Chapter 6
Basic Operations

This chapter describes the SANWatch screen elements and basic operations.

- **Starting SANWatch Agents – Section 6.1, page 6-3**
- **Starting SANWatch Manager – Section 6.2, page 6-4**
  - **6.2.1 Locally or via LAN under Windows 2000/ 2003 Environments**
  - **6.2.2 Locally or via LAN under Linux Environments**
  - **6.2.3 Locally or via LAN under Solaris Environments**
  - **6.2.4 For Remote Management via Web Browser (Any Supported OSes)**
- **Start Using SANWatch Manager – Section 6.3, page 6-6**
  - **6.3.2 Connecting to a RAID Subsystem**
  - **6.3.3 Using the Agent List Window**
  - **6.3.4 Disconnecting and Refreshing a Connection**
- **Security: Authorized Access Levels – Section 6.4, page 6-13**
- **Look and Feel – Section 6.5, page 6-14**
  - **6.5.1 Look and Feel Overview**
  - **6.5.2 Screen Elements**
  - **6.5.3 Command Menus**
  - **6.5.4 Outer Shell Commands**
  - **6.5.5 Management Window Commands**
- **The Array Information Category – Section 6.6, page 6-18**
  - **6.6.1 Enclosure View**
  - **6.6.2 Tasks Under Process Window**

- **6.6.3 Logical Drive Information Window**
- **6.6.4 Logical Volume Information Window**
- **6.6.5 Fibre Channel Status Window**
- **6.6.6 System Information Window**
- **6.6.7 Statistics Window**

♦ **The Maintenance Category – Section 6.7, page 6-22**

- **6.7.1 Logical Drive Maintenance Window**
- **6.7.2 Physical Drives Maintenance Window**
- **6.7.3 Task Schedules Maintenance Window**

♦ **The Configuration Category – Section 6.8, page 6-28**

- **6.8.1 Quick Installation**
- **6.8.2 Installation Wizard**
- **6.8.3 Create Logical Drive Window**
- **6.8.4 Existing Logical Drives Window**
- **6.8.5 Create Logical Volume Window**
- **6.8.6 Existing Logical Volumes Window**
- **6.8.7 Channel Window**
- **6.8.8 Host LUN Mapping Window**
- **6.8.9 Configuration Parameters Window**

♦ **Arranging Windows – Section 6.9, page 6-33**

♦ **Multi-array Management – Section 6.10, page 6-35**

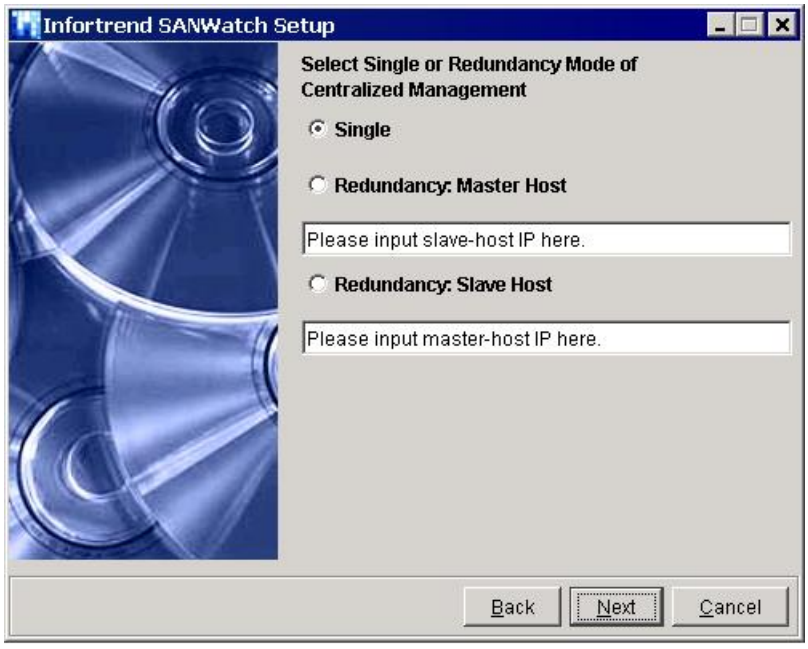
6.1 Starting SANWatch Agents

Once the SANWatch software is properly installed, the necessary software agents start automatically each time the management station is started or reset, e.g., RAID Agents and Root Agents. However, the GUI part of SANWatch and the Configuration Client utility need to be manually started.

Since the majority of RAID storage applications require non-stop operation, the Configuration Client utility, which is used to monitor and report array conditions, should be installed on a management server that runs 24-7 operation. For a higher level of fault tolerance in case of server failure, the Configuration Client can be installed on more than one server. As shown below, when installing SANWatch using the Advanced/Centralized Management scheme, a pair of redundant servers can be specified in the installation wizard prompt. The configuration is done by specifying IP addresses for a Master Host and a Slave Host.

IMPORTANT!

To make use of the server redundancy feature, SANWatch must be manually installed (Advanced Installation, and then choose Mode 1 installation: Centralized Management) onto both the Master and Slave hosts. The Configuration Client functionality on a stand-by Slave host becomes active only when the Master host fails.



Before management can be performed on a particular disk array system, you need to first establish a connection from your array to the network or a connection between your array and the directly attached server. Once a connection is established, management can be started.

The following discusses how to connect to a disk array. Information on disconnection is provided at the end of this section.

6.2 Starting SANWatch Manager

The management software interface, SANWatch Manager, needs to be started by a network or RAID subsystem manager regardless of which OS is being used.

Depending on your setup, you can start SANWatch Manager in various ways.

For both local and remote management, and under various OSes, starting the program is simple. Please refer to the appropriate sub-sections below for information.

6.2.1 Locally or via LAN under Windows 2000/ 2003 Environments

From the Startup menu, select Programs → Infortrend Inc. → SANWatch Manager. (See ***Figure 6-1***.) Double-click the SANWatch Manager icon.

Figure 6-1: SANWatch Shortcuts on Windows Startup Menu

- OR -

Double-click the SANWatch Manager icon from the desktop (see ***Figure 6-2***) if a shortcut was added during the installation process.

Figure 6-2: SANWatch Shortcut on Windows Desktop

6.2.2 Locally or via LAN under Linux Environments

To startup SANWatch manager under Linux environments, follow the steps below:

Step 1. After the main program of SANWatch manager is installed, the SANWatch program files can be located under the following directory (default): /usr/local/Infortrend Inc/RAID GUI Tools.

Step 2. To execute SANWatch manager, type: ./sanwatch.sh in the terminal screen.

Step 3. To open configuration client, type: ./configuration.sh in the terminal screen

6.2.3 Locally or via LAN under Solaris Environments

To startup SANWatch manager under Solaris environments, follow the steps below:

Step 1. After the SANWatch program is completely installed, the SANWatch files can be found on the path /usr/local/Infortrend Inc/RAID GUI Tools.

Step 2. Type ./sanwatch.sh to launch SANWatch program.

Step 3. Type ./configuration.sh to open Configuration Client.

6.2.4 For Remote Management via Web Browser (Any Supported OSes)

Step 1. Start your web browser and enter the IP address assigned to the RAID subsystem Ethernet port or that of a RAID-attached server as your URL (e.g., 210.212.121.123). The IP of a RAID-attached server is used when the server uses **in-band** protocols to communicate with the attached RAID array. After a brief delay while the Java Applet starts, the SANWatch Manager main connection wizard appears on the screen.

Step 2. The SANWatch management window should start after a brief moment.

NOTE:

In Applet mode, connecting to the second array requires opening another browser window and entering its IP.

6.3 Start Using SANWatch Manager

When the SANWatch Manager is launched, A **SANWatch Connection** window will first prompt and appear on the screen.

During the time the management software is initializing, a SANWatch initialization page displays.

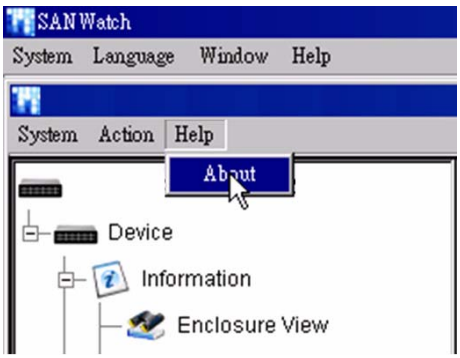
Infortrend SANWatch®
GUI Manager for EonStor® Disk Array Subsystems
Copyright© 1999~2005 Infortrend Technology, Inc. All rights reserved.
Infortrend

A single click on the initial screen brings out a **Connection Abort** confirm box. You can end a connection before the management console is established.

6.3.1 Beginning the Trial Use of the Data Service

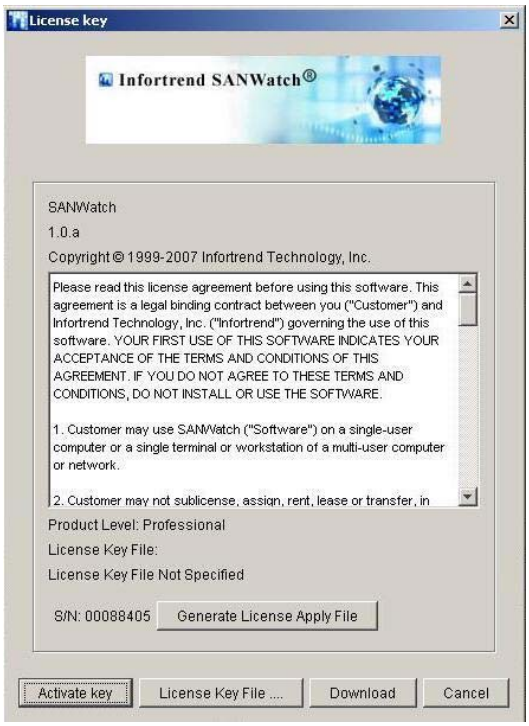
The **License Key** window automatically prompts the first time you start a SANWatch console. You may activate the trial use or activate later using the **Help** -> **About** button.

An ordinary SANWatch console will not display the **Data Service** options unless you enable the trial use.



To begin using the Data Service, click on **Help** (one on the management console with a RAID system, not that on the outer shell window), and the **About** button to display the **License key** window.

SANWatch comes with a 30 days trial period for its Data Service functionality. After the 30 days trial, you should proceed with purchasing the software to continue the use of the Data Service (Snapshot) functionality.


License key
Infortrend SANWatch®
SANWatch
1.0.a
Copyright © 1999-2007 Infortrend Technology, Inc.
Please read this license agreement before using this software. This agreement is a legal binding contract between you ("Customer") and Infortrend Technology, Inc. ("Infortrend") governing the use of this software. YOUR FIRST USE OF THIS SOFTWARE INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT INSTALL OR USE THE SOFTWARE.
1. Customer may use SANWatch ("Software") on a single-user computer or a single terminal or workstation of a multi-user computer or network.
2. Customer may not sublicense, assign, rent, lease or transfer, in
Product Level: Professional
License Key File:
License Key File Not Specified
S/N: 00088405
Generate License Apply File
Activate key
License Key File ....
Download
Cancel

For a **trial use**, proceed with one of the following:

- For an enclosure that comes with SANWatch-compatible firmware (e.g., FW3.61), a trial key is available in the backplane EEPROM. Simply click on the **Activate key** button to begin trial use.

- For an enclosure running older firmware (e.g., FW3.48), you need to upgrade firmware and proceed with applying for a trial key or the licensed use. For more details, please refer to **Chapter 15**.

NOTE:

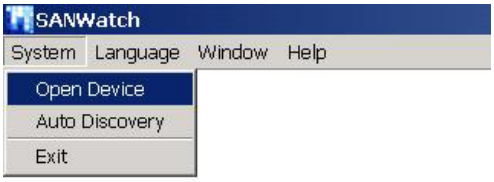
If the software becomes expired and you already created Snapshot volumes, these Snapshot Container volumes will return to the state of ordinary logical drives after a system reset.

6.3.2 Connecting to a RAID Subsystem

The following steps will explain how to connect to a RAID Subsystem through a network connection.

Step 1. A **Connection** window appears when the SANWatch software is started. If you have a specific RAID array's IP address in mind and wish only to manage one array, simply enter the IP address to proceed.

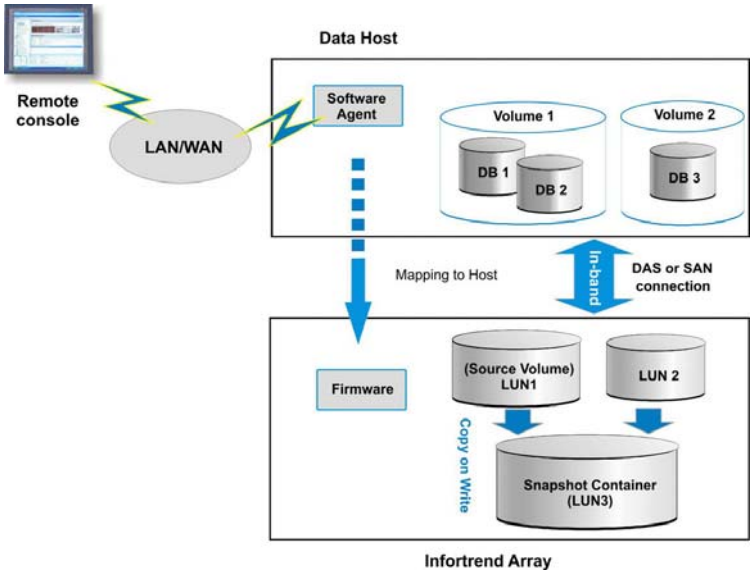
On the computer screen, if you can not see the SANWatch **Connection** window, it can be opened from the SANWatch program menu. Click on the **System** and then select **Open Device** command, and the **SANWatch Connection** window will prompt.



NOTE:

The **Data Service** (Snapshot) functionality of SANWatch Professional version is available with the following configurations:

1. You manage a RAID array using SANWatch from on a DAS (Direct-Attached Storage) server.
2. SANWatch is installed **both** on a DAS server and a remote management computer. SANWatch runs on a remote computer making access to a data host which has a Flush Agent running for Snapshot protection. Enter the IP address of the data host. The access to the RAID array is made via Infortrend's proprietary, intermediate software agent. The intermediate software agent then communicates with the array firmware via the in-band protocols over the existing host-storage data links.



3. If you enter the RAID system's Ethernet IP, you will not have the flush agent support and not able to utilize the Snapshot **Scheduler** utility.

Step 2. As soon as you input the first number of an IP address, the screen will show the previous entries. You can select a previously connected address on the pull-down menu.

NOTE:

If you are not sure of a RAID array's IP address, you may rely on the **Auto Discovery** option in the **Configuration Client** to automatically detect the available RAID arrays that are controlled by root agents. If the **Auto Discovery** option is enabled, the available RAID arrays will be shown in the Agent List window that is described later in this section. To use the **Auto Discovery** option, please refer to Section 4.5: Auto Discovery.

Step 3. You may select to enable the **Secure Sockets Layer** (**SSL**) security option by a single mouse-click on its check box. SSL works by using a private key to encrypt data when transmitting private documents and obtain confidential information. SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely.

Step 4. Enter a user name by selecting from the pull-down menu. Each user name represents an authorized access level. Enter a password to proceed. Leave it blank if there is no preset password. Click the **OK** button to start the management session.

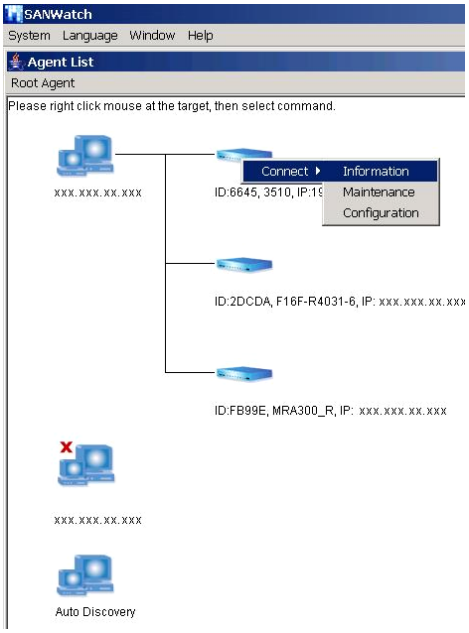
NOTE:

Refer to Section 6.4 for the details of the three authorized access levels.

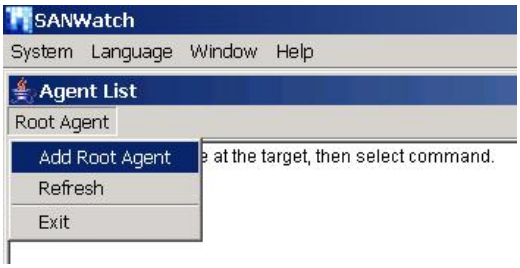
6.3.3 Using the Agent List Window

A unique **Agent List** window is memorized by the SANWatch Manager to help you search available RAID subsystems that are connected to the network or a specific root agent. To use the Agent List window, please follow the steps below:

Step 1. If you would like to see the available RAID subsystems that are connected to the network or a specific root agent, you may click the **Show Root Agent List** button on the bottom of the SANWatch **Connection** window. The window displays the tree tables of the available RAID systems that are detected by the **Auto Discovery** function. An example of an Agent List window is shown below.



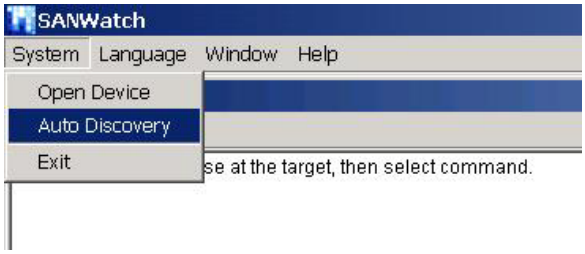
Step 2. If you like to add a new root agent, single-click on the **Root Agent** command menu in the Agent List window and select **Add Root Agent**. Enter a root agent IP address in the address prompt. Any RAID systems that are managed through the intermediate root agent will be shown in a tree table in the Agent List window.



Step 3. You may refresh the devices displayed on the **Agent List** window by selecting **Refresh** under the Root Agent command menu.

Step 4. Click on the controller/subsystem that you want to manage and select an authorized access level. Enter any necessary password and the program will lead you to its management session.

Step 5. If you like the system to search the available RAID systems again, pull down the **System** command menu and select **Auto Discovery**. The new search result will be displayed in the Agent List Window.



When the system is searching for Root Agents on the network, the Auto Discovery option in the System pull-down menu will be temporarily disabled.

NOTE:

The **Auto Discovery** details are described in ***Chapter 4, Section 4.5: Auto Discovery.***

6.3.4 Disconnecting and Refreshing a Connection

From the **System** menu, select **Logout**.

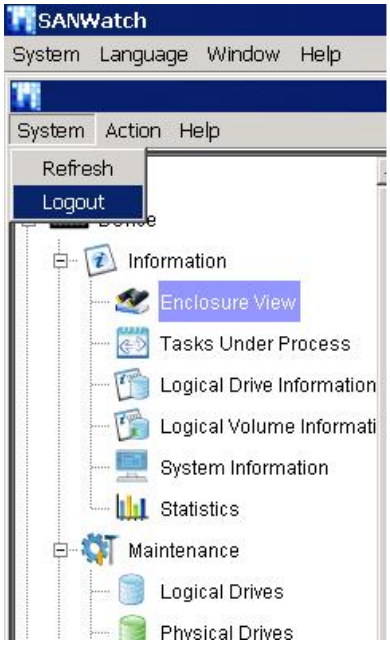


Figure 6-3: Ending a Management Session with a Connected Array

Select **Logout** will close the current management session and return to the **Outer Shell** window. If you wish to connect to another RAID array, enter its IP address and then click ***OK*** to proceed. Click ***Cancel*** to close the connection prompt and return to the **Outer Shell** window.

Selecting the **Refresh** button allows you to re-connect with an array if a RAID system has been temporarily disconnected; e.g., the RAID system is being reset or the host links were disconnected for maintenance reasons.

6.4 Security: Authorized Access Levels

Password protection is implemented with the Connection wizard to prevent unauthorized access to configured arrays. This protection, which is implemented along with the security access levels, prompts a user for the station password the first time he or she attempts to connect to a RAID system.

By default, no password is required to access a RAID system using the first two protection levels, "**Configuration**" (Administrator) and "**Maintenance**" (User). A default password is required for the **Information** login.

Default Passwords	
Configuration	Password previously set for the controller/ subsystem; press **Enter** for none. The password can be changed in "Configuration Parameters" window in SANWatch's main program.
Maintenance	You can configure a password for this level login in "**Configuration Parameters**" window in SANWatch's main program.
Information	Default password is "**1234**."

It is recommended to configure passwords for the first two access levels at the first time you successfully connect to an array. **Information** users can monitor array status and see event messages. A user logging for **Maintenance** access can perform maintenance jobs onto configured arrays, and a user logging in using the **Configuration** login has full access to create, modify, or delete all related array configurations.

Note that some RAID subsystem/controllers may have been configured with a password using terminal or LCD keypad utilities. This preset password can be used for a "Configuration" login. However, the password can be changed using "Configuration Parameters" window in SANWatch's main program. See ***Chapter 7*** for the description of password setup.

6.5 Look and Feel

6.5.1 Look and Feel Overview

Because SANWatch Manager is a Java-based GUI program, it accommodates the "look-and-feel" standards of various Operating Systems. At present, the Windows interface appearance is supported.

SANWatch Manager will auto-detect and configure to match the OS where it is currently running.

In the event of a compatibility problem or under an unknown OS or OS versions, the program will default to the Java look and feel.

Just like other GUI-based applications, the SANWatch Manager works entirely with windows, buttons, and menus to facilitate various disk array operations. These windows follow the standard Windows look-and-feel specifications, so that manipulating elements and windows within any SANWatch Manager window generally conforms to standard procedures. The management sessions are best displayed with 1024x768 screen resolution.

NOTE:

Screen captures throughout this document show the Windows look and feel.

6.5.2 Screen Elements

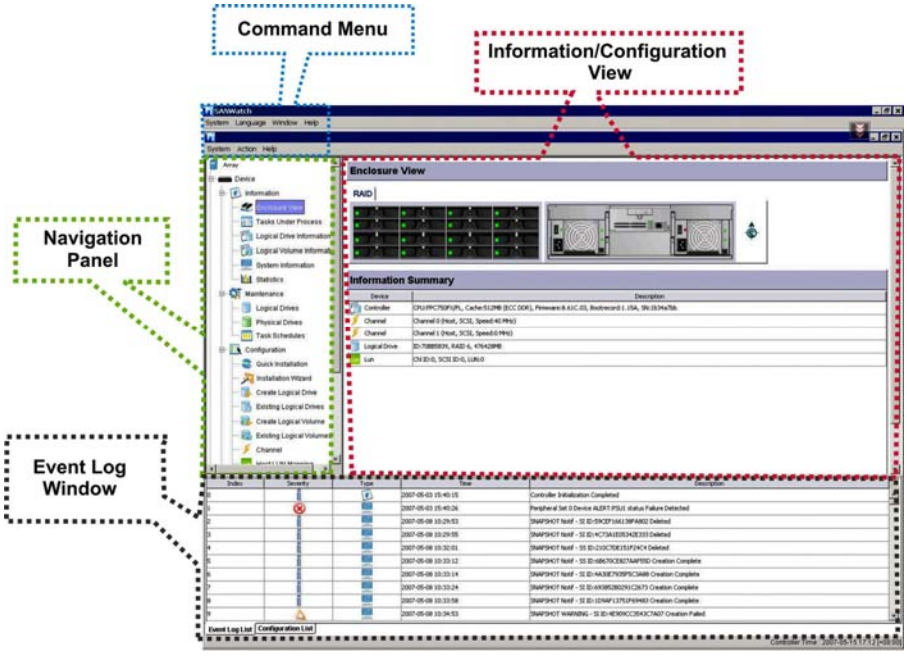


Figure 6-4: GUI Screen Elements

The GUI screen can be divided mainly into three (3) separate windows: a tree-structure **Navigation Panel**, the **Information/Configuration** window, and the **Event Log/Configuration View** window at the bottom.

Each information or configuration window can also be accessed through the command menus on the upper left corner of the management interface. At the bottom of the Event Log window, tab buttons allow you to switch the view to the Configuration View display.

6.5.3 Command Menus

The menu bar (shown in ***Figure 6-5)*** displays the available menus on the Outer Shell window. The Outer Shell window contains multiple management windows each providing access to a connected array.

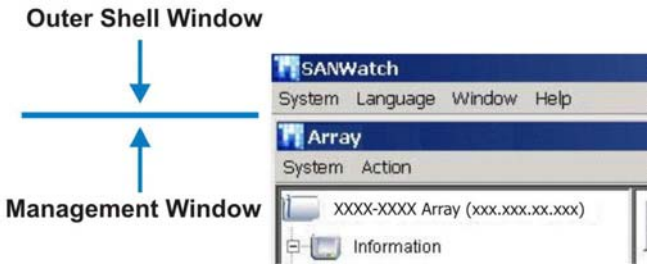


Figure 6-5: Command Menu Bar

All menus provide a list of commands for invoking various disk array and display-related operations.

For a summary of commands, see ***Appendix A,*** *Command Summary*.

NOTE:

Multiple simultaneous SANWatch Managers can connect to one RAID subsystem.

6.5.4 Outer Shell Commands

The following commands are described in ***Section 6.5.2*** and shown in ***Figure 6-6***.

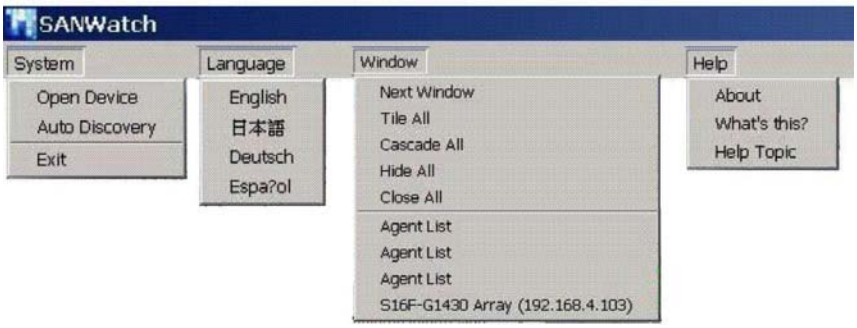


Figure 6-6: Outer Shell Commands

- Under **System** menu, the **Open Device** command lets you connect to a RAID array. This command triggers the connection prompt. Multiple arrays can be managed each in a separate management window.

  Click the **Auto Discovery** command will start a new search of any available RAID systems in the specific IP ranges on the network. The function can be setup using Configuration Client utility.

  The **Exit** command under the **System** menu is always available and is used to end all SANWatch Manager sessions at once.

- The **Language** items allow you to display the on-screen GUI, instructions, commands, messages, and explanatory legends in a different languages. The current supporting languages are **English**, **Deutsch, Spanish** and **Japanese**.

- The **Window** command allows you to enlarge, shrink or rearrange the system view window(s). Please refer to ***6.9 Arranging Windows*** for details on the use of the Window commands.

- Under the **Help** menu, the **About** command displays a window that provides SANWatch version and copyright information.

  The **Help Topic** commands displays the online help contents, which are implemented in Java Help format.

  You may click the **What's this?** command, move it around the screen, and display related information by a second mouse-click on the screen element you are interested in.

6.5.5 Management Window Commands

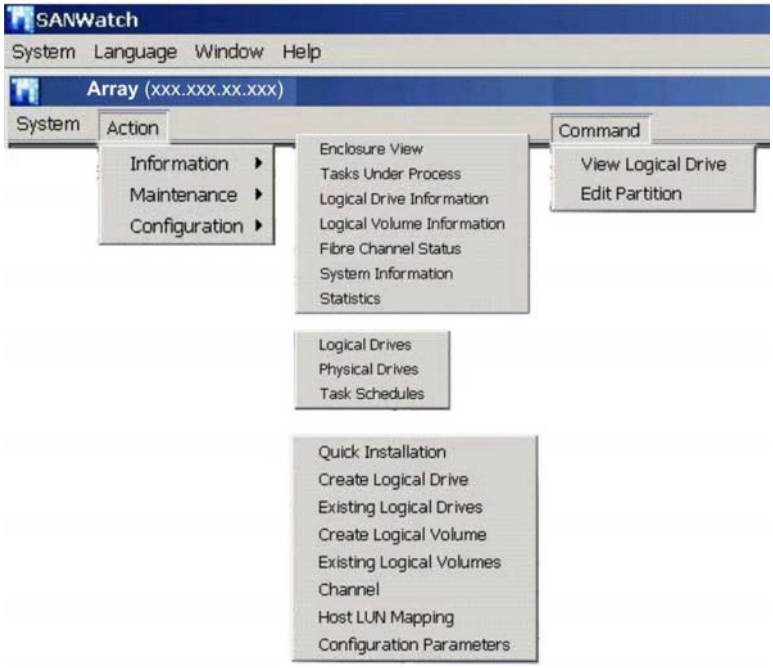
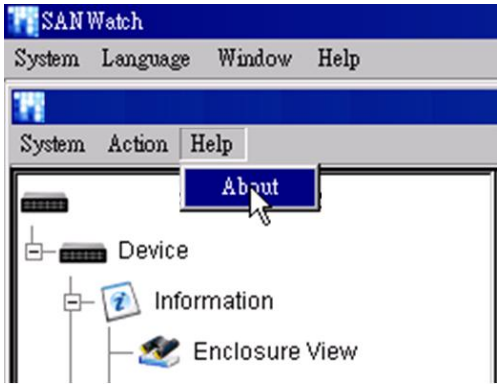


Figure 6-7: Management Window Commands

- The **Refresh** command sends instructions to the GUI asking to review the connection status. The **Logout** command under the **System** menu allows you to disconnect from a controller/subsystem and to end the software session. This command is only available when SANWatch Manager is currently connected to a RAID array.

- The **Action** menu brings up sub-menus that allow you to access various options under the three (3) configuration categories: **Information**, **Maintenance** and **Configuration**. Each of these options will be discussed later in this chapter.

- The **Command** menu provides different configuration options only when specific configuration items are selected in a functional display window. On the other hand, when a configurable item is selected, the corresponding command menu and the related commands automatically appear on the menu bar.



- **Help:** The **About** button under the Help menu enables you to activate the trial use of the Data Service functionality or open a License key window for purchasing the SANWatch Data Service functionality.

6.6 The Information Category

The **Information** category allows you to access to information about every aspect of system operation.

To access the information category, either select the icon from the navigation tree or go to the **Action** Command menus and then select **Information** on the top of the screen.

Figure 6-8: Accessing Information Commands

6.6.1 Enclosure View Window

The **Enclosure View** window displays the physical view of all major components, including drive slots and enclosure components. When the Enclosure View window is opened, the screen below should appear. Use the Enclosure View window to monitor multiple enclosures from the computer screen. For details of using the Enclosure View window, please refer to ***Chapter 12***.

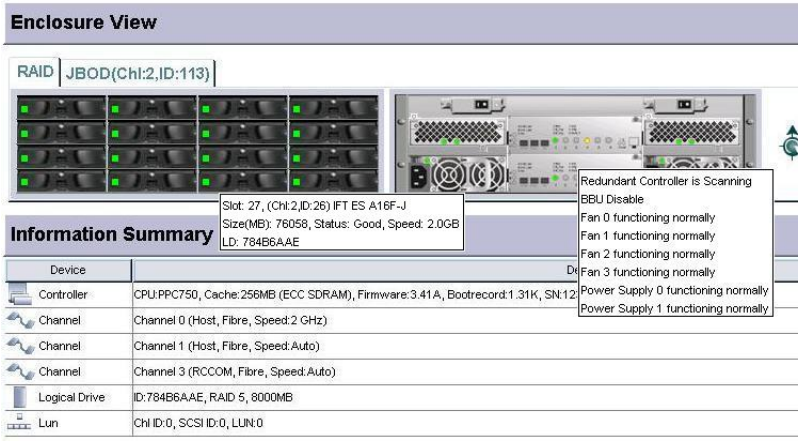


Figure 6-9: Enclosure View Window

6.6.2 Tasks Under Process Window

The **Tasks Under Process** window (shown in ***Figure 6-10)*** reminds you of unfinished tasks being processed by a subsystem. The start time and percentage of progress are also displayed on-screen.

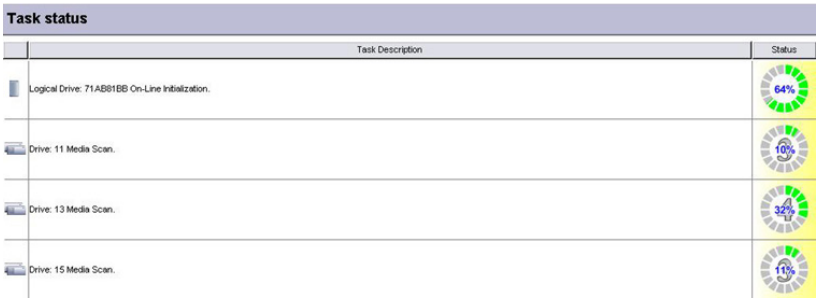


Figure 6-10: Task Status Window

6.6.3 Logical Drive Information Window

The **Logical Drive Information** window provides the configuration, management, and monitoring functions available in SANWatch. The Logical Drive View window includes three (3) sub-windows: **Logical Drive Status**, **Front View**, and **Logical Drive Message**.

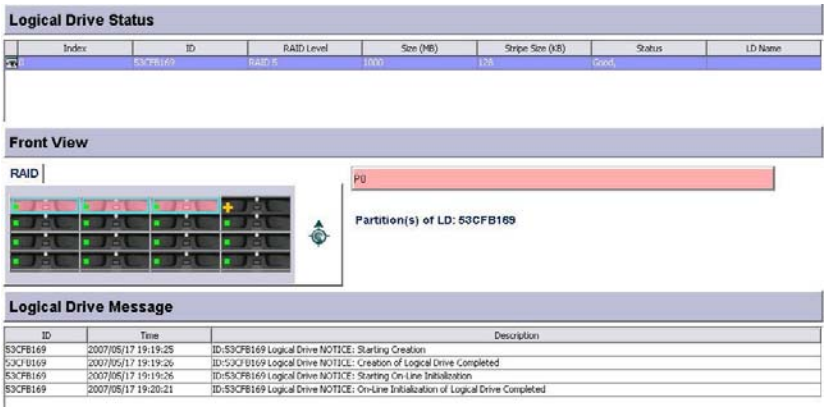


Figure 6-11: Logical Drive information

Logical Drive Status: This sub-window displays information on configured arrays (logical drives) showing a unique array ID, RAID level, capacity, array status and a name that can be manually assigned.

Front View: This sub-window helps you to quickly identify configured arrays by the physical locations of their members. Different arrays are distinguished by different colors. When any member drive is selected by a mouse click the rest of the array's members will be highlighted by bright blue lines, indicating they are members of the selected array.

Formation of logical partitions is displayed next to the Front View window.

Logical Drive Message: Messages related to a selected array are automatically listed at the bottom of the screen.

6.6.4 Logical Volume Information Window

The **Logical Volume Information** window provides the configuration of a configured volume. The Logical Volume Information window includes three sub-windows: Logical Volume Status, Member Logical Drive(s), and Related Information.

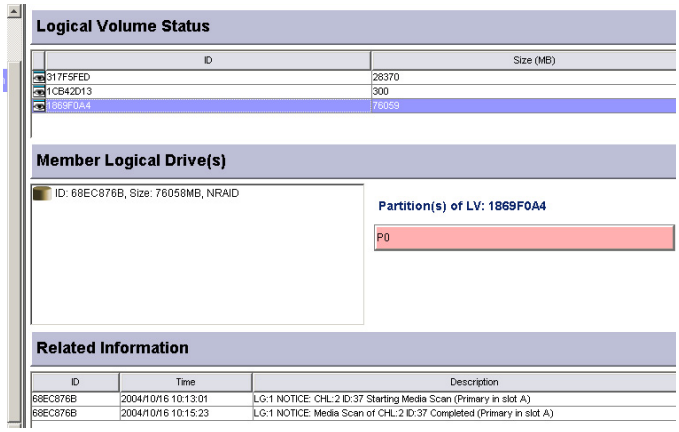


Figure 6-12: Logical Volume Information

6.6.5 Fibre Channel Status Window

The **Fibre Channel Status** window displays information on the Fibre host channel ID, connection speed, host-side connection protocols (topology), link status, WWPN port name and WWNN node name, loop IDs, and Fibre Channel address. The corresponding icon turns gray and is disabled if SANWatch operates with a SCSI or iSCSI host subsystem. This information is useful when configuring a subsystem for a heterogeneous environment such as a storage network operating with multiple hosts and applications.

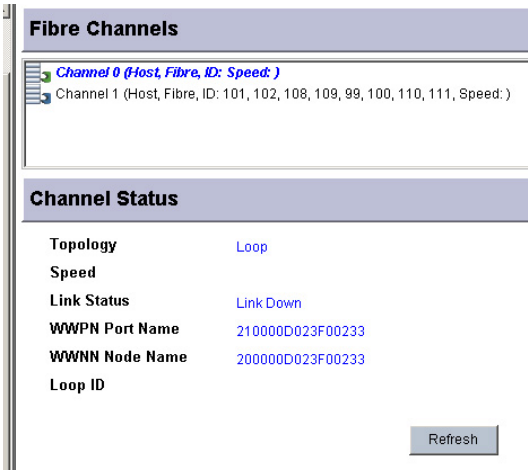


Figure 6-13: Fibre Channel Status Window

6.6.6 System Information Window

The **System Information** window provides key information about the RAID subsystem and the RAID controller unit that powers the subsystem. Enclosure information includes the operating status of power supply,

temperature sensors, and cooling fan units. Controller information includes CPU, firmware/boot record version, serial number, CPU and board temperature, voltage, and status of the battery backup module. This window has no configuration options.

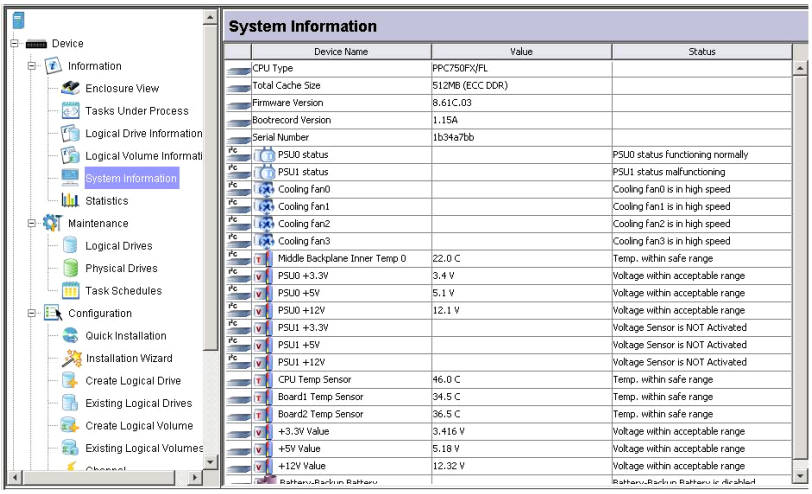


Figure 6-14: System Information Window

6.6.7 Statistics Window

Select the **Statistics** window in the configuration tree, and start calculating "Cache Dirty" rate or "Disk Read/Write Performance" by clicking either or both of the check boxes.

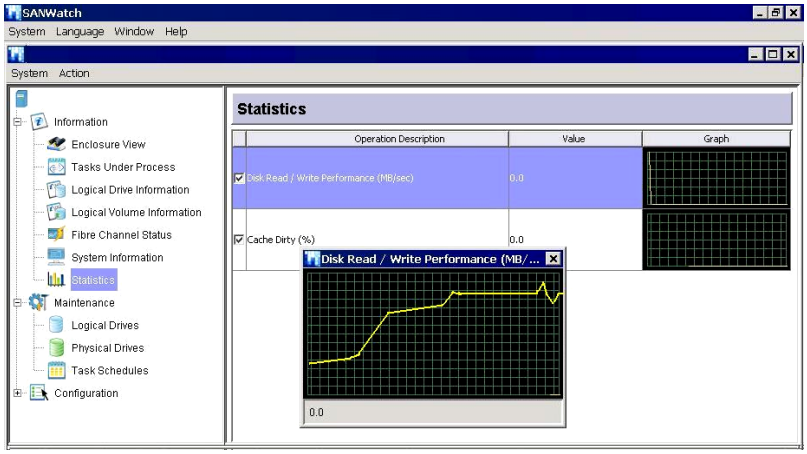


Figure 6-15: Performance Statistics Window

A double-click on the performance graph will bring out a larger performance window.

Cache Dirty (%)

If you select Cache Dirty (%) check box, a window similar to the one shown above will appear. The percentage of the cache blocks in use is displayed in numbers and the cache hits average is displayed as a graph. The Cache Dirty rate provides cached writes data over the last few minutes and indicates data caching consistency and frequency.

Disk Read/Write Performance (MB/s)

If you select Disk R/W Performance check box, a statistic window will appear showing the read/write performance. A real-time view of current activity is provided as a graph and the performance data is constantly updated and displayed as MB/s.

6.7 The Maintenance Category

The **Maintenance** category provides access to logical and physical drives and performs maintenance functions that help ensure the integrity of the configured arrays. The operation of the Maintenance window also includes access through the Navigation Panel and a functional window.

To access the maintenance category, either select the icon from the navigation tree or go to the **Action** command menus and then select **Maintenance** on the top of the screen.

Figure 6-16: Accessing Maintenance Commands

6.7.1 Logical Drive Maintenance Window

When the **Logical Drives** maintenance window is opened, the screen shown below will appear.

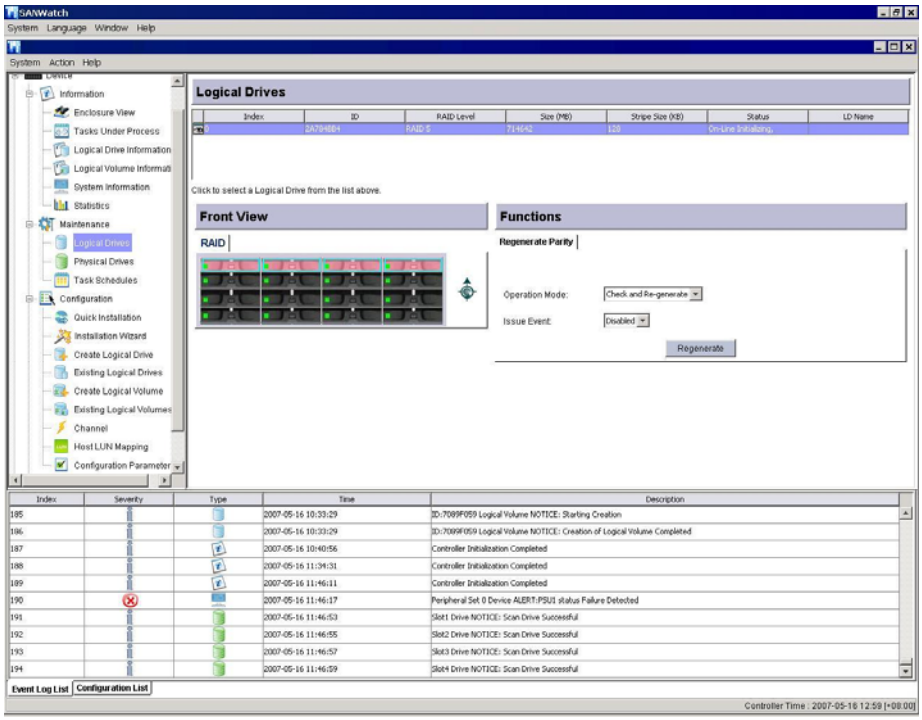


Figure 6-17: Maintenance - Logical Drives

There are three (3) sub-windows in the Logical Drives maintenance mode window:

- The **Logical Drives** window provides a list of all configured arrays. Use a single mouse-click to select the logical drive you wish to perform the maintenance tasks on.

- The **Front View** window allows you to see the locations of the members of logical drives. Note that a logical drive is selected by a single mouse-click from the list of configured arrays on the upper half of the screen.

- The **Functions** window provides configuration options for maintenance tasks and buttons, which start a maintenance task.

  - **Media Scan** - Media Scan examines drives and detects the presence of bad blocks. If any data blocks have not been properly committed and defects are found during the scanning process, data from those blocks are automatically recalculated, retrieved and stored onto undamaged sectors. If bad blocks are encountered on yet another drive during the rebuild process, the block LBA (Logical Block Address) of those bad blocks will be shown. If rebuild is carried out under this situation, rebuild will continue with the unaffected sectors, salvaging the majority of the stored data.

    There are two options with performing the Media Scan:

Operation Priority: determines how much of the system resources will be used for the drive scanning and recalculating process.

Operation Mode: determines how many times the scan is performed. If set to "continuous," the scan will run in the background continuously until it is stopped by a user.

The system can automatically perform a Media Scan according to a preset task schedule. For more details, please refer to ***Section 6.7.3***.

- **Regenerate Parity** - If no verifying method is applied to data writes, this function can often be performed to verify parity blocks of a selected array. This function compares and recalculates parity data to correct parity errors.

NOTE:

The function is available for logical drive with parity protection, one that is configured to RAID level 1, 3, 5 and 6.

- **Rebuild** – To manually rebuild a logical drive. When this feature is applied, the controller will first examine whether there is any Local Spare assigned to the logical drive. If yes, it will automatically start to rebuild.

  If there is no Local Spare available, the controller will search for a Global or Enclosure Spare. If there is a Global Spare, logical drive rebuild will be automatically conducted.

6.7.2 Physical Drives Maintenance Window

When the **Physical Drives** maintenance window is opened, the below screen will appear.

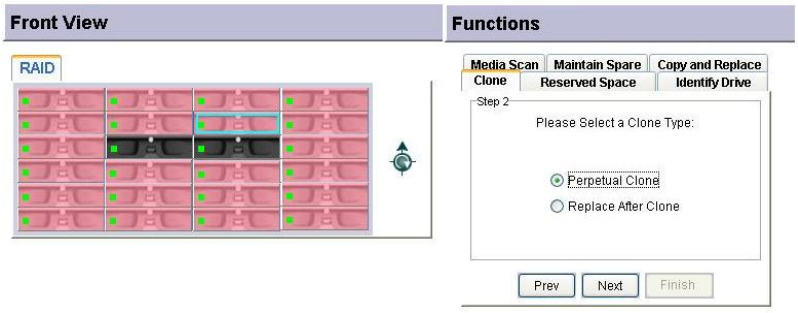


Figure 6-18: Maintenance - Physical Drives

There are two (2) sub-windows in the Physical Drives maintenance window:

- The **Front View** window allows you to select a hard drive to perform maintenance tasks on. A selected drive is highlighted by bright blue lines, and its slot number is shown in the **Functions** window in the **Selected Drive Slot** field.

- The **Functions** window provides configuration options with maintenance tasks and an **APPLY** or **Next** button to apply the configuration.

  - **Media Scan** – You can perform the Media Scan function to a specific physical drive. To start a media scan, select a disk drive from the **Front View** window then select one of the tabbed menus in the **Functions** window and click the **Apply** button.

  - **Maintain Spare** – You can add a spare drive from the list of the unused disk drives. The spare chosen here can be selected as a **Global** or **Local** spare drive. If you choose to create a Local spare drive, select a logical drive from the enclosure view on the left. Click **Next** to move to the next screen. Click **Finish** to complete the configuration process. A manual rebuild function is also available here if a failed drive has just been replaced.

NOTE:

A logical drive composed in a non-redundancy RAID level (NRAID or RAID 0) does not support spare drive rebuild.

  - **Copy and Replace** – Logical drives can be expanded by copying and replacing the member drives with drives of higher capacity. The data blocks or parity data on an array member is copied onto a new drive, and then the original member can be removed. Once all members are replaced by larger drives, the added capacity will appear as a new logical partition.

    NOTE that to perform the **Copy and Replace** function, you must have an unused drive slot for the replacement drive, e.g., by temporarily disabling a Spare drive.

  - **Clone** – a system administrator can also choose to manually perform the "**Clone Failing Drive**" function on an individual disk drive.

  - **Reserved Space** – The 256MB reserved space can be removed from a disk drive once a drive member is excluded from a logical drive. The reserved space, a space formatted with a micro-file system, can be manually removed from a "used drive."

- **Identify Drive** – Use this function to identify a drive on the subsystem. Administrations can identify an individual drive in a configuration consisting of multiple arrays by forcing its LEDs to flash. Select a disk drive from the **Front View** window, select one of the flash drive options, and then click on the **Apply** button in the **Functions** window.

- **Scan/Add/Clear Drive** – The **Scan drive** function allows users to scan in a newly added disk drive from a channel bus. The **Add** and **Clear** function only appears when you click on an empty drive slot on a Fibre and SCSI drive channel RAID subsystem. The feature enables users to manually add a drive entry when the drive slot is empty. The created entry can be deleted by applying the **Clear Drive Status** option.

- **Low Level Format** – This function only appears with a new disk drive which has not been configured into a RAID array. This function allows you to perform a low-level format on a new disk drive.

- **Read/Write Test** – You can perform a read/write test onto a single disk drive. Click on the disk drive that you wish to test in the **Front View** window and then set the test conditions, such as **Error Occurrence** and **Recovery Process**, in the **Functions** window. Click **Apply** to start the action.

6.7.3 Task Schedules Maintenance Window

The **Physical Drives** maintenance window is shown below:

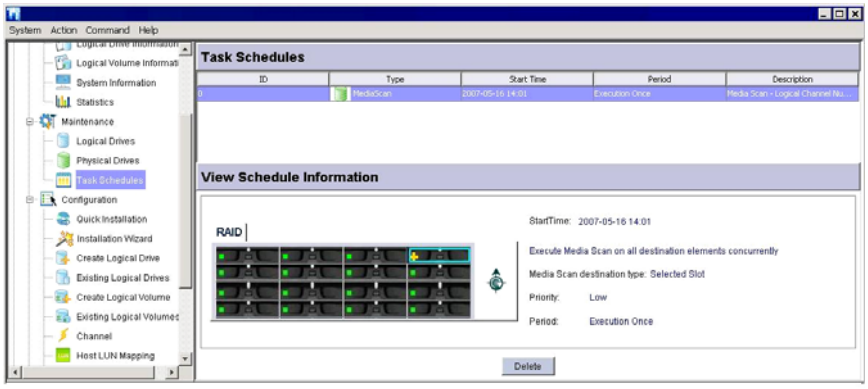
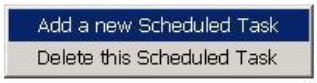


Figure 6-19: Task Schedules Window

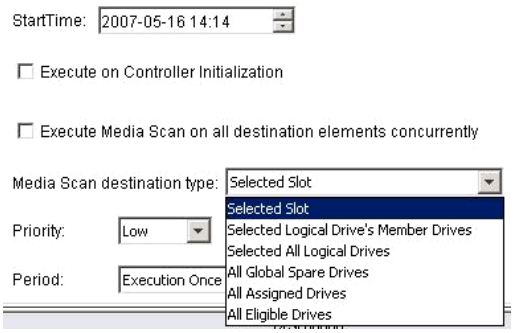
To begin using the Task Schedule functionality, right-click to display the **Add a New Scheduled Task** command.



There are two (2) sub-windows in the **Task Schedules** window:

- The **Task Schedules** window displays previously configured schedules that are now being held in NVRAM.

- The **Add a New Task Schedule** window allows you to select a hard drive or logical drive to perform a scheduled task on. Before you make the selection by mouse-clicks, select a scan target from the **Media Scan destination type** pull-down list.



A selected disk drive or a logical drive is highlighted by a bright blue square and its related options are displayed in check boxes, dropdown list, or vertical scroll bars.

- The **Add** button at the bottom of the screen allows you to complete the process and add the task schedule.

6.8 The Configuration Category

The **Configuration** category contains functional windows that allow you to create logical configurations and set appropriate configuration settings for system operations. This category is available only when logging in using the **Configuration** access with the correct password.

To access the **Configuration** category, either select the respective icon from the navigation tree or go to the **Action** command menus and then select the **Configuration** functions from the menu bar.

Figure 6-20: Accessing Configuration Commands

6.8.1 Quick Installation

When you first connect SANWatch to a new RAID system without any previous configurations, select **Quick Installation** and let SANWatch guide you through a simple logical drive creation process. When created, the logical drive is automatically mapped to the first available host ID/LUN.

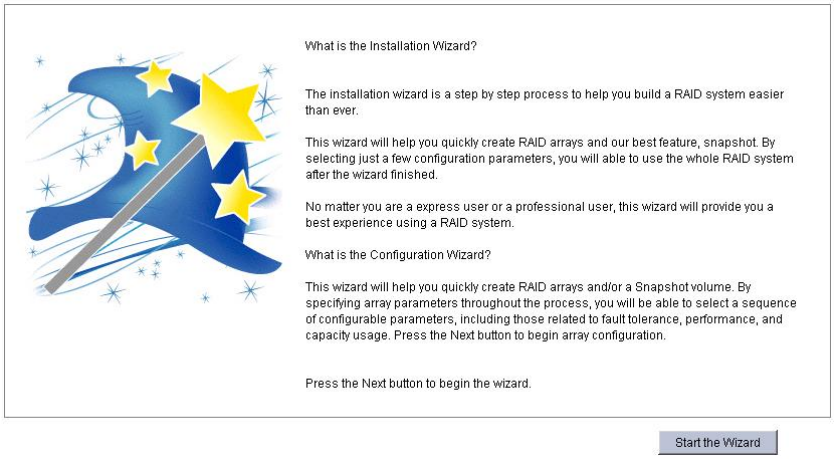
NOTE:

The **Quick Installation** function includes all disk drives in **ONE** big logical drive and makes it available through one host ID/LUN, which may not be the best choice for all RAID applications especially for large enclosures with multiple host ports and those consisting of many disk drives.

If you already have at least one logical drive in the RAID subsystem, this function will automatically be disabled. You will be prompted by a message saying a logical drive already exists.

6.8.2 Installation Wizard

The installation wizard comes with step by step instructions and choices that help you quickly configure your RAID systems and snapshot protection.


What is the Installation Wizard?
The installation wizard is a step by step process to help you build a RAID system easier than ever.
This wizard will help you quickly create RAID arrays and our best feature, snapshot. By selecting just a few configuration parameters, you will able to use the whole RAID system after the wizard finished.
No matter you are a express user or a professional user, this wizard will provide you a best experience using a RAID system.
What is the Configuration Wizard?
This wizard will help you quickly create RAID arrays and/or a Snapshot volume. By specifying array parameters throughout the process, you will be able to select a sequence of configurable parameters, including those related to fault tolerance, performance, and capacity usage. Press the Next button to begin array configuration.
Press the Next button to begin the wizard.
Start the Wizard

6.8.3 Create Logical Drive Window

When the **Create Logical Drive** window is opened, the screen shown in ***Figure 6-21*** will appear.

The basic rules for using the functional elements in the Create Logical Drive window are:

- This window uses a parallel display principle. To create a logical drive, select its members from the Front View window each by a single mouse-click. The **Selected Members** window then displays the disk drives' slot IDs and sizes.

- The creation screen also employs an up-then-down pattern with the configuration process. Important logical drive characteristics are set using the dropdown lists at the lower part of the configuration screen. The creation procedure is completed by clicking the **OK** button at the bottom of the screen.

- A selected physical drive is highlighted by a bright blue square; a second mouse-click on it deselects the disk drive.

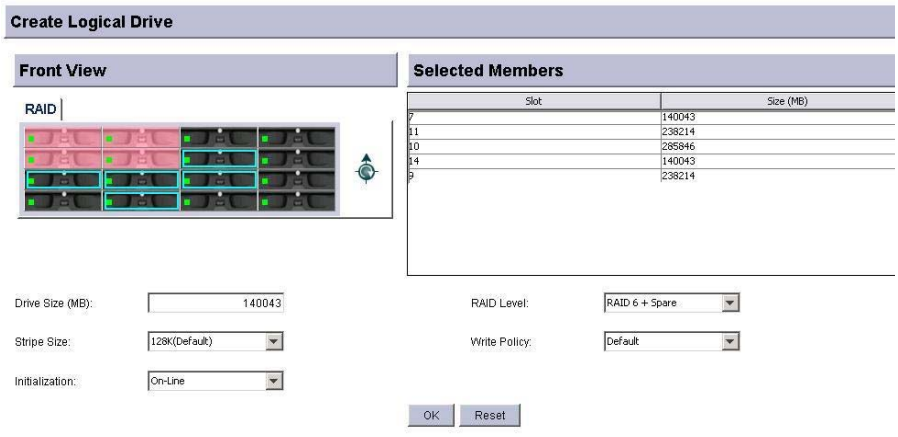


Figure 6-21: Selecting Members for a New Logical Drive

For details on creating a logical drive, please refer to ***Chapter 9*** of this document.

6.8.4 Existing Logical Drives Window

When the **Existing Logical Drives** window is opened, the screen shown in ***Figure 6-22*** will appear.

The basic rules for using the functional elements in the Existing Logical Drives window are:

- This window also uses a parallel display and the up-then-down principle. To start configuring an existing array, select a configured array from the LD list above. Locations of its members are automatically highlighted, and then the available functions are displayed in the **Functions** window.

- This window contains three or four edit commands that can be triggered by a right-click on a configured array.

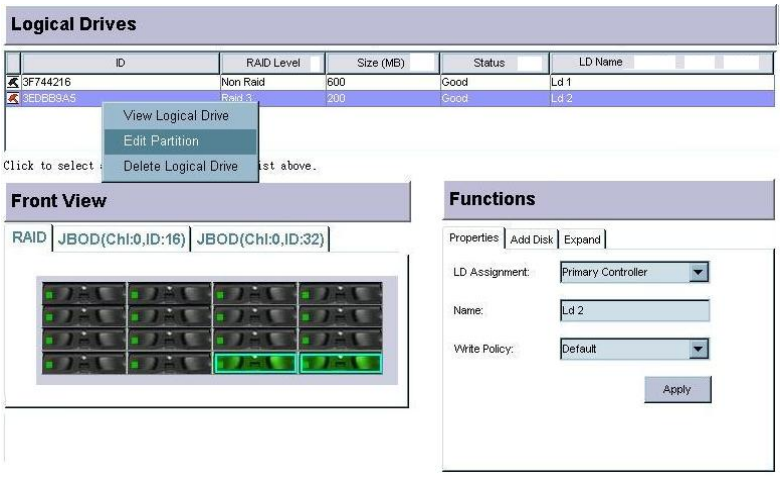
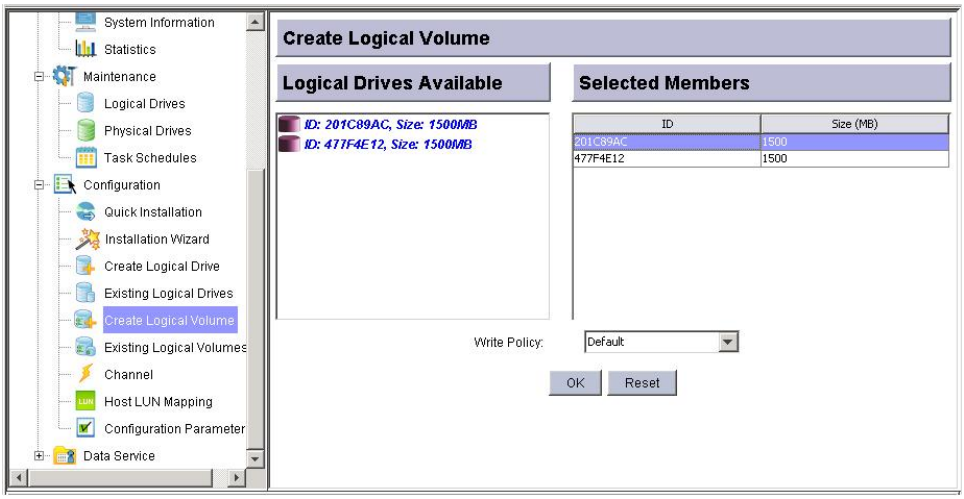


Figure 6-22: Existing Logical Drives Window

6.8.5 Create Logical Volume Window

This window uses the same operation flow as that applied in the Create Logical Drive window. A Logical Volume contains one or more Logical Drives, and these members are striped together.

To create a Logical Volume, first select its members from the **Logical Drives Available** column, selected members will appear on the right. Note that because members are striped together, it is recommended that all members included in a Logical Volume contain the same drive size. You may then select the **Write Policy** specific to this volume and click **OK** to finish the process or click **Reset** to restart the configuration process.



6.8.6 Existing Logical Volumes Window

This window uses the same operation flow as that applied in the Existing Logical Volumes window.

NOTE:

This window also contains Edit mode commands that are only accessible by a mouse right-click.

6.8.7 Channel Window

The **Channel** window allows you to change host or drive port data rate**,** channel mode (EonStor 2510FS only), and to add or remove channel IDs.

Two pages, **Parameters** and **ID**, display on the right of the **Channel** screen.

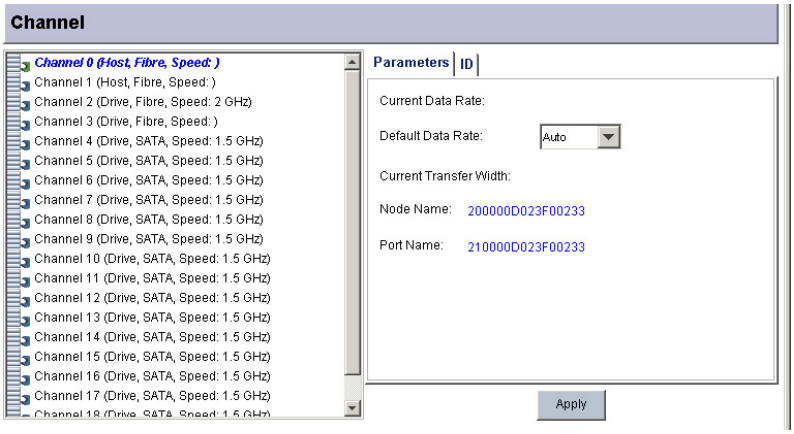

Channel
Channel 0 (Host, Fibre, Speed:)
Channel 1 (Host, Fibre, Speed:)
Channel 2 (Drive, Fibre, Speed: 2 GHz)
Channel 3 (Drive, Fibre, Speed:)
Channel 4 (Drive, SATA, Speed: 1.5 GHz)
Channel 5 (Drive, SATA, Speed: 1.5 GHz)
Channel 6 (Drive, SATA, Speed: 1.5 GHz)
Channel 7 (Drive, SATA, Speed: 1.5 GHz)
Channel 8 (Drive, SATA, Speed: 1.5 GHz)
Channel 9 (Drive, SATA, Speed: 1.5 GHz)
Channel 10 (Drive, SATA, Speed: 1.5 GHz)
Channel 11 (Drive, SATA, Speed: 1.5 GHz)
Channel 12 (Drive, SATA, Speed: 1.5 GHz)
Channel 13 (Drive, SATA, Speed: 1.5 GHz)
Channel 14 (Drive, SATA, Speed: 1.5 GHz)
Channel 15 (Drive, SATA, Speed: 1.5 GHz)
Channel 16 (Drive, SATA, Speed: 1.5 GHz)
Channel 17 (Drive, SATA, Speed: 1.5 GHz)
Parameters
ID
Current Data Rate:
Default Data Rate:
Auto
Current Transfer Width:
Node Name:
200000D023F00233
Port Name:
210000D023F00233
Apply

Figure 6-23: Channel Window

On the **Parameters** page, channel mode, current data rate, default data rate and current transfer width are displayed.

Channel Mode: Only applicable on the EonStor 2510FS series. This option allows you to change the I/O channel operating mode. The channel mode selections can be: host, drive, RCC, drive +RCC.

Default Data Rate: Should only be applied with limitations on current configuration, e.g., when network devices (optical cables and adapters) are running on different speeds.

The **ID** page allows you to add or remove IDs by selecting or deselecting ID boxes.

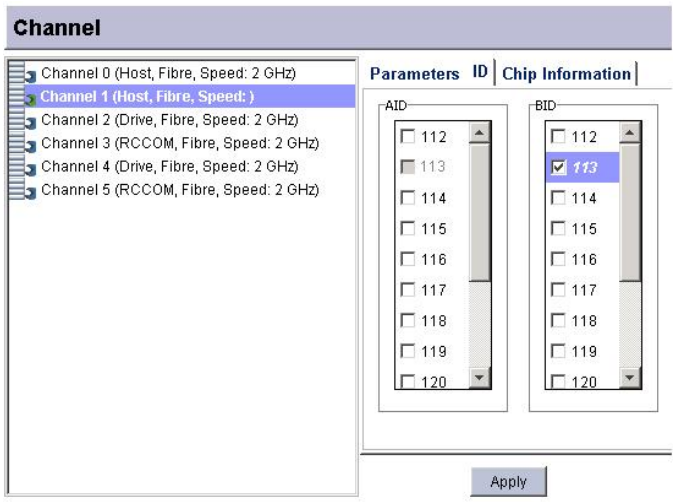


Figure 6-24: Host Channel ID Settings

Be sure to click ***Apply*** for the configuration to take effect. For details of how to configure channel-related settings, please refer to ***Chapter 8*** of this document.

NOTE:

Changing the channel mode or adding/removing IDs requires resetting the controller/subsystem.

6.8.8 Host LUN Mapping Window

The **Host LUN Mapping** window allows you to associate configured arrays with host channel IDs or LUN numbers.

- The Host LUN Mapping window contains four sub-windows: Host LUN(s), WWN Names(s), and Logical Drive(s) or Volume(s).
- This window also contains a right-click menu that creates association with either a Primary Controller (Slot A) ID or a Secondary Controller (Slot B) ID.

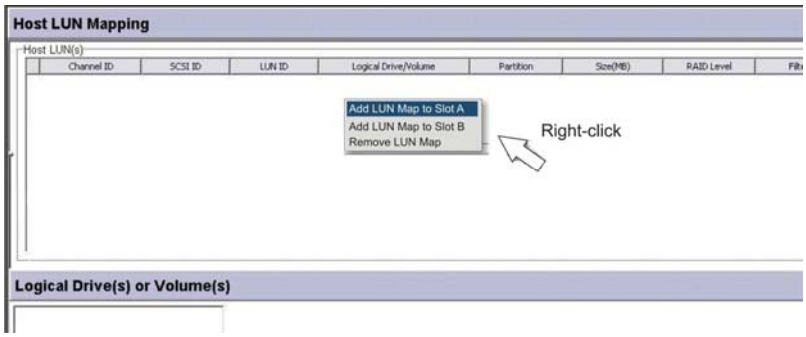


Figure 6-25: Host LUN Mapping Right-click Menu

6.8.9 Configuration Parameters Window

The Configuration Parameters window allows you to change various system preference options.

This window uses tabbed panels to provide access to the functional sub-windows. Each sub-window provides configurable options using check boxes, check circles, drop down boxes, or pull-down menus. Clicking the **Apply** button will complete the configuration process. A mixture of message prompts, file path windows, text fields, and confirm boxes ensure ease of use. Refer to ***Chapter 7*** for details of each configuration options.

6.9 Arranging Windows

Each array configuration window is enveloped in a system view window. The **system view window** is the area where you interact with SANWatch program. You can select commands from the outer shell **Window** menu to enlarge, shrink, or rearrange the currently opened system view(s) on your screen. You may also select each connected system by clicking the listed systems at the bottom of the **Window** menu.

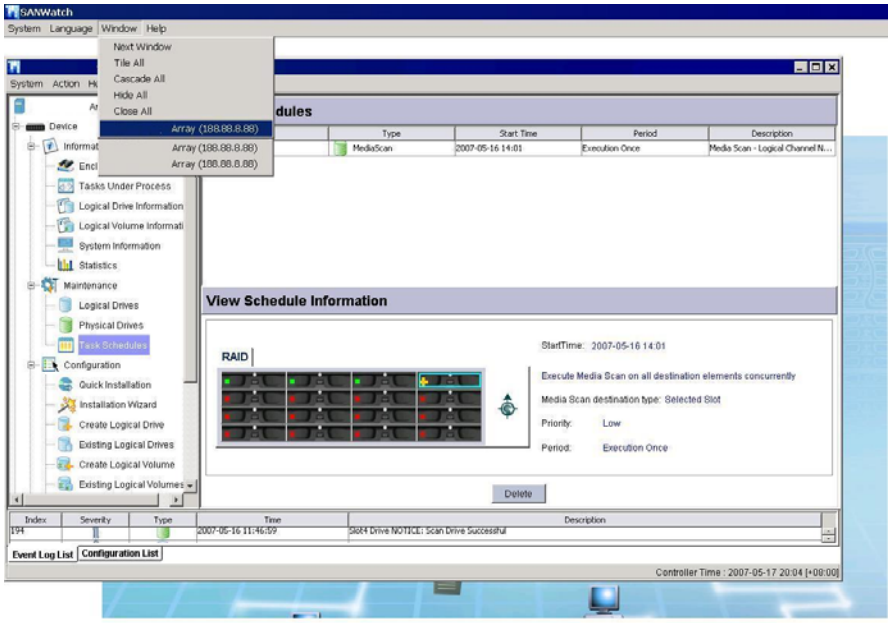


Figure 6-26: The "Outer Shell" System View Window

The window menu includes the following commands:

- **Next Window:** The Next Window command change which window is active. The active window is raised to the top of the screen. If you connect more than one RAID system, this command allows you to switch between different system view windows. The Next Window command is useful if you want to circulate through all the windows on the screen.

- **Tile All:** Use the Tile All command to arrange and display all system view windows. This allows you to view multiple systems simultaneously.

- **Cascade All:** Use the Cascade All command to diagonally arrange and display all system view windows on the screen. This allows you to view multiple systems at a glance.

- **Hide All:** When you select this command, all active system view windows will be minimized to small icons on the bottom left of the SANWatch screen. To enlarge the system view window, click on the icon(s).

- **Close All:** If you select this command, all the RAID systems will be disconnected and every system view windows will be closed.

- **System List:** A list of the connected RAID systems is shown in the Window menu. To view a specific system, a single click on the system name will display its system view window.

6.10 Multi-array Management

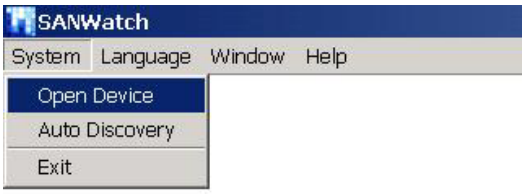


Figure 6-27: Opening Device for Multi-Array Management

Management of multiple arrays is allowed by clicking the **Open Device** command under the **System** menu. The **Exit** command ends the SANWatch manager session with all configured arrays. Clicking the **Open Device** command and the connection wizard is followed. Multiple management windows can be opened.

NOTE:

If you need to open multiple console windows, it is recommended you have at least 512MB or more memory on your management station.

This page is intentionally left blank.

Chapter 7

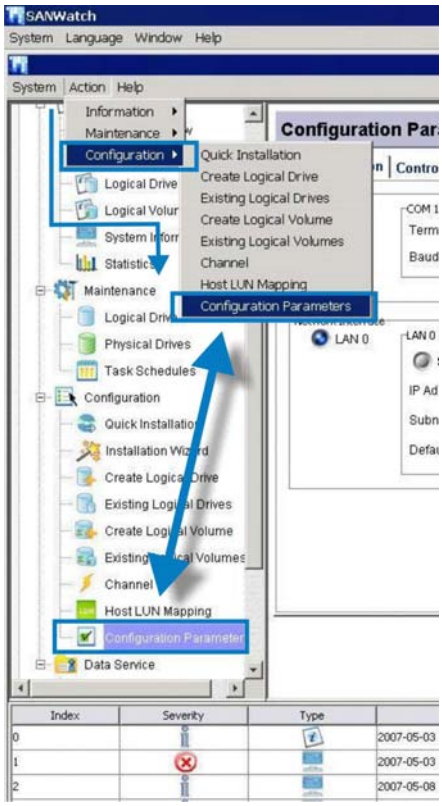
Configuration Parameters

SANWatch Manager enables you to modify the configuration of the disk array controller from your manager console. This chapter describes the following configuration features:

- **Accessing Configuration Parameters Options - Section 7.1**
- **Communications – Section 7.2**
- **Controller – Section 7.3**
- **System – Section 7.4**
- **Password – Section 7.5**
- **Threshold – Section 7.6**
- **Redundant Controller Settings - Section 7.7**
- **Event Triggered Operations – Section 7.8**
- **Other - Section 7.9**

7.1 Accessing the Configuration Parameters Options

To access controller configuration options, either use the Configuration category icons on the Navigation Tree or select the Configuration Parameters command from the command menu to open the **Configuration Parameters**. The configuration window contains many options that are directly related to array performance, and should be configured ***before*** creating logical arrays.

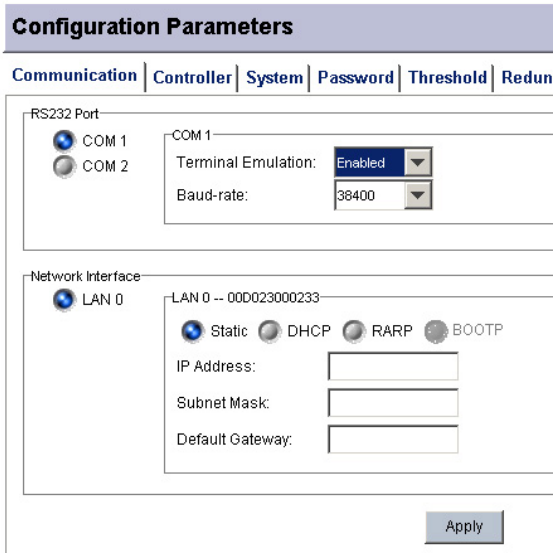


The following is a complete list of configuration controls and optional menus that you will have available once the **Configuration Parameters** option has been selected.

More information about many of these variables is available in the controller hardware and firmware documentation.

7.2 Communications

To configure the **Communication** options, select the **Communication** page from the **Configuration Parameters** window.



RS-232C Port

Infortrend RAID subsystems/controllers come with one or two serial ports. Before proceeding with configuration, first select COM1 or COM2 by a single mouse click.

- **Terminal emulation** allows you to enable or disable the terminal emulation option. If you want to connect the COM port to a computer running terminal emulation, enable the option and set the identical baud rate to the computer COM port.

- **Baud rate** allows you to control the serial port baud rate. Select an appropriate value from the pull-down menu.

Network Interface

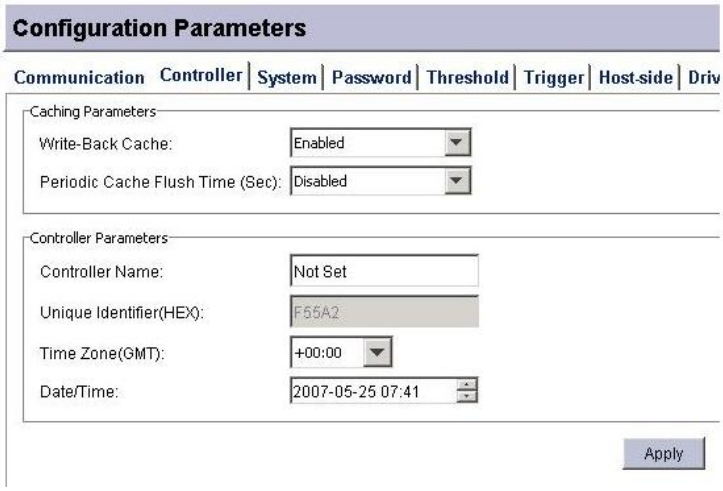
Depending on your network setting, select a protocol selection circle to obtain adequate TCP/IP support. This column is used to configure the subsystem's Ethernet port. If the **Static** box is selected, consult your network administrator for appropriate IP address, subnet mask and gateway values.

Click **Apply** for the configurations to take effect.

7.3 Controller

"Controller" here refers to the RAID controller unit, which is the main processing unit of a RAID subsystem. The configuration window contains two sub-windows: "Caching" and "Controller Parameters." To configure the

controller's caching behaviors, select an appropriate value from each of the pull-down menus.



The data cache can be configured for optimal I/O performance using the following variables:

Caching Parameters

- **Write-Back Cache**

  - **Enabled, Host Writes are cached before being distributed to hard drives**. This improves write performance but requires battery backup support to protect data integrity in case of a power outage.

  - **Disabled, Cache Write-Through.** Used primarily if no cache battery backup is installed and if there is increased likelihood of a power failure.

  - **Default.** This value is considered as a "**Not-specified**" option. If set to default, the subsystem's caching mode will be automatically adjusted especially when the event triggered operation has been configured. For example, if a cooling module fails, the subsystem firmware automatically switches caching mode to the conservative Write-through.

- **Periodic Cache Flush Time**

  This option allows you to select the desired interval for the subsystem to flush cached data. This applies especially with subsystems that come without BBU support.

Controller Parameters

- **Controller Name**

A manually entered nickname for the RAID controller. This name can also be used to recognize a RAID subsystem in an environment where multiple RAID subsystems reside.

- **Unique Identifier (HEX)**

  This is a ***MUST*** for subsystem configuration, especially for those with dual-controllers or Fibre host ports. The unique ID is integrated as unique Fibre Channel node name and port names. In the event of controller failover and failback, this ID helps host-side initiators to identify a RAID subsystem.

- **Time Zone(GMT)**

  GMT (Greenwich Mean Time) is used with a 24-hour clock. To change the clock to your local time zone, select a time from the drop-down menu. Choose the hour later than the Greenwich Mean Time following a plus (+) sign. For example, enter "+9" for Japan's time zone.

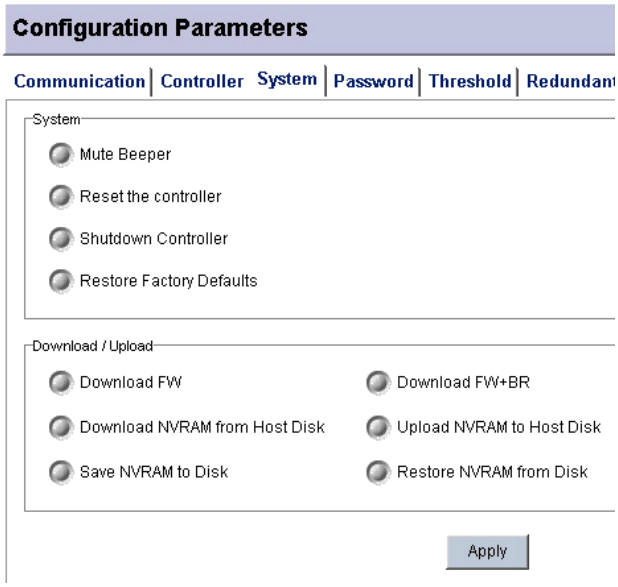
- **Date/Time**

  Enter time and date in their numeric representatives in the following order: month, day, hour, minute, and the year.

When preferences have been set with the configurations above, click **Apply** to make the changes.

7.4 System

To access the System-specific functions, select the **System** page, as shown in below, from the **Configuration Parameters** window.



Each function is executed by a two-step procedure. Click the select button of the function you wish to perform and click the "**Apply**" button for the configuration to take effect.

Select only one option each time from the **System** page. You may repeat the steps if you like to proceed with more than one option.

System Functions

- **Mute Beeper.** Turns the beeper off temporarily for the current event. The beeper will still be activated by the next event. Be sure that you have checked carefully to determine the cause of the event.

- **Reset Controller.** Resets the subsystem without powering off.

- **Shutdown Controller.** This prepares the subsystem to be powered off. This function flushes the unfinished writes still cached in controller memory making it safe to turn off the subsystem.

- **Restore Factory Default.** When you apply this function, any settings that you have made in SANWatch program will be formated and the original factory default configuration will be restored.

WARNING!

Restore Factory Default will erase all your array preferences, including host ID/LUN mappings. Although the configured arrays remain intact, all other caching or performance-specific options will be erased.

If configured arrays cannot be properly associated with host ID/LUNs, data inconsistency might occur.

It is best to save your configuration details before using this function.

Download/Upload

- **Download FW.** Subsystem firmware can be upgraded using the existing management connection (whether Ethernet or in-band). Provide the firmware filename using the file location prompt. SANWatch will start to download the firmware. Find an appropriate time to temporarily stop the access from host systems, then reset the controller in order to use the new downloaded firmware.

NOTE:

Do not use this command to download license key for the advanced Data Service functionality. The license key download is accessed through the license key pop-up window.

- **Download FW+BR:** This allows you to download the firmware and boot record together. It may not be necessary to upgrade the boot record each time you update your firmware binaries. Please refer to the readme text file that came with each firmware version.

- **Download NVRAM from Host Disk:** The subsystem configuration is saved in NVRAM and can be saved to a system drive. This function allows you to retrieve a previously saved configuration profile from a system disk.

NOTE:

All of the download functions will prompt for a file source from the current workstation.

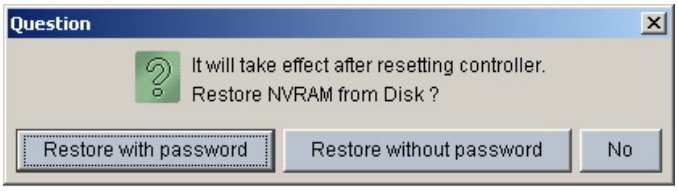
- **Upload NVRAM to Host Disk:** This allows you to backup your controller-dependent configuration information to a system drive. We strongly recommend using this function to save the configuration profile whenever a configuration change is made.

- **Save NVRAM to Disk:** The configuration profile can also be saved to array hard drives. Each array hard drive will have a replica of the NVRAM backup in its reserved space so that when a drive fails or is being regrouped, the backup remains intact.

- **Restore NVRAM from Disk:** If an administrator wishes to retrieve the previously saved NVRAM backup from subsystem hard drives, all settings including system password will also be restored. With these option, an administrator can decide whether to restore previous

configuration using the original password just in case you forget the original password.

A question window will prompt showing the options.



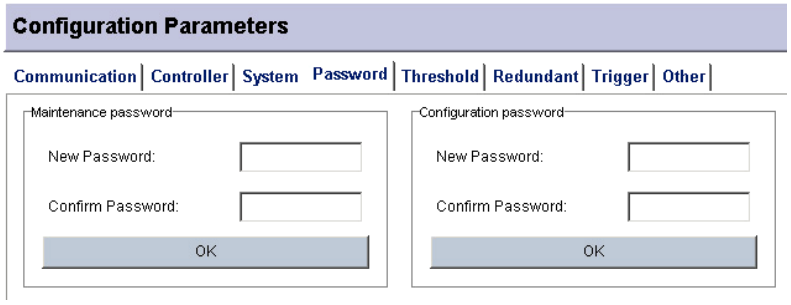
NOTE:

Upload NVRAM will prompt for a file destination at the current console.

This option is only available in Firmware revision 3.47 or above.

7.5 Password

To configure different levels of the Access authorization **Password**, select the **Password** page from the **Configuration Parameter** window.



Maintenance Password

Users logging in using the Maintainance Password will be able to access the first two configuration categories, Information and Maintenance. You may set the Maintenace Password here and click **OK** for the change to take effect.

Configuration Password

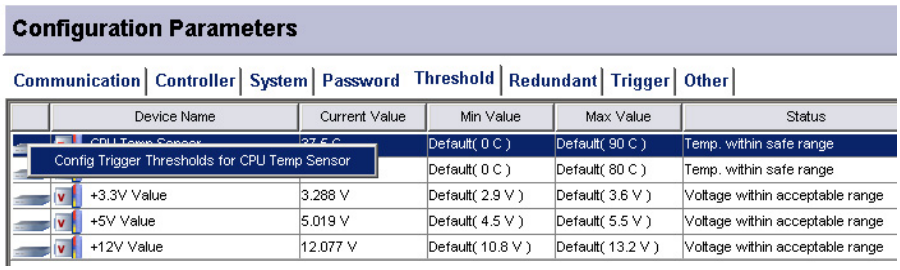
Users logging in using the Configuration Password have full access to all configuration options. A super-user has the right to access all three configuration categories on the navigation tree. You may set the Configuration Password here and click **OK** for the change to take effect.

7.6 Threshold

To access the event **threshold** options, click the **Threshold** page in the **Configuration Parameters** window.

This window allows you to change the preset values on thresholds used to monitor the condition of the RAID controller unit(s) in your subsystem. For example, these threshold values can be changed if the controller operates in a system enclosure where the upper or lower limit on ambient temperature is much higher or lower than that on the RAID controller. Adjusting the default thresholds can coordinate the controller status monitoring with that of the system enclosure.

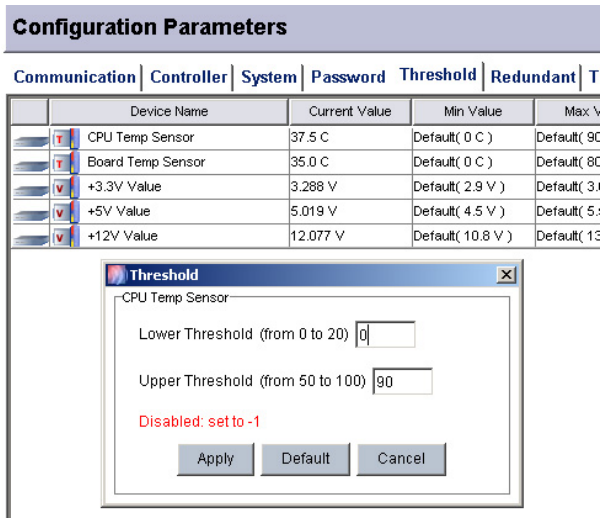
It is not recommended to change the threshold values unless extreme conditions are expected on the installation site.



To change the threshold values on a specific monitored item, for example, the CPU Temp Sensor, right-click on the item. The **Configuration** button will prompt. Left-click on the **Configuration** button to bring up the **threshold** window.

WARNING!

The upper or lower thresholds can also be disabled by entering "-1" in the threshold field. However, users who disable the thresholds do this at their own risk. The controller(s) will not report condition warning when the original thresholds are exceeded.



You may then enter a value in either the lower or upper threshold field.

NOTE:

If a value exceeding the safety range is entered, an error message will prompt and the new parameter will be ignored.

Click **Apply** for the configuration change to take effect.

Click **Default** to restore the default values for both thresholds.

Click **Cancel** to cancel this action and go back to the Threshold page in the **Configuration Parameters** window.

7.7 Redundant Controller Settings

This sub-window contains **configuration** options related to redundant controller configurations. This **Redundant** page only displays if your controller/subsystem comes with dual-redundant RAID controllers.

Each option is executed by a two-step procedure. Click to select a desired value from the pull-down menu, and then click **Apply** for the configuration to take effect.

- **Secondary Controller RS-232 Terminal:** In a redundant controller configuration, the RS-232C port on the Secondary controller is normally nonfunctional. Enable this function if you wish to use the port for debugging purposes.

NOTE:

Access to the Secondary controller only allows you to see controller settings. In a redundant-controller configuration, configuration changes have to be made through the Primary controller.

- **Periodic Cache Flush Time:** If redundant controllers work with Write-Back caching, it is necessary to synchronize the unfinished writes in both controllers' memory. Cache synchronization lets each controller keep a replica of the unfinished writes on its partner, so that if one of the controllers fails, the surviving controller can finish the writes.

  If controllers are operating using the Write-Through caching mode, the **Periodic Cache Flush Time** can be manually disabled to save system resources and achieve better performance.

NOTE:

If the **Periodic Cache Flush** is disabled, the configuration changes made through the Primary controller is still communicated to the Secondary controller.

- **Adaptive Write Policy:** Firmware is embedded with intelligent algorithms to detect and to adapt the array's caching mode to the I/O requests characteristics. The capability is described as follows:

1. When enabled, the adaptive write policy optimizes array performance for sequential writes.

2. The adaptive policy temporarily disables an array's write-caching algorithm when handling sequential writes. Write-caching can be unnecessary with sequential writes so that write requests can be more efficiently fulfilled by writing data onto disk drives in the order in which they are received.

3. The adaptive policy changes the preset write policy of an array when handling I/Os with heterogeneous characteristics. If the firmware determines it is receiving write requests in a sequential order, the write-back caching algorithm is disabled on the target logical drives.

   If subsequent I/Os are fragmented and received randomly, the firmware automatically restores the original write-cache policy of the target logical drives.

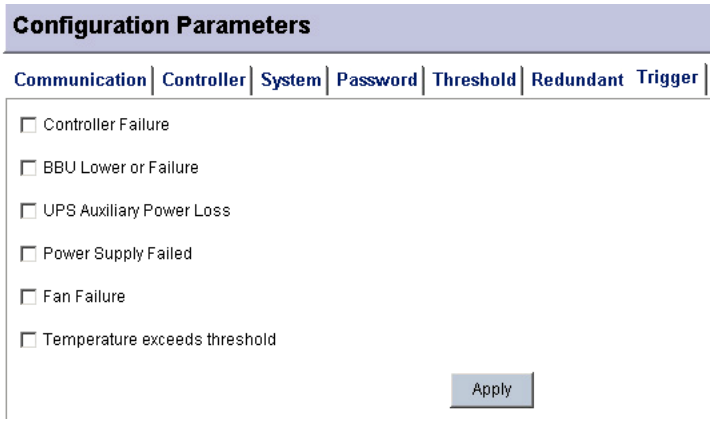
   Adaptation for Redundant Controller Operation

4. If arrays managed by a redundant-controller configuration are configured to operate with write-back caching, cached data will be constantly synchronized between the partner controllers. Synchronization consumes system resources. By disabling synchronization and write-back caching, the direct writes to system drives can be more efficient. Upon receiving sequential writes, the firmware disables write-back caching on target arrays and also the synchronized cache operation.

IMPORTANT!

The **Adaptive Write Policy** is applicable to subsystems working under normal conditions. In the degraded conditions, e.g., if a drive fails in an array, the firmware automatically restores the array's original write policy.

7.8 Event Triggered Operations



To reduce the chance of data loss caused by hardware failure, the controller/subsystem can automatically commence an auto cache flush upon the detection of the following conditions. When cache contents are forced to be distributed to hard drives, the Write-Back caching mode is also switched to the Write-Through mode.

1. Controller Failure
2. BBU Lower or Failure
3. UPS Auxiliary Power Loss
4. Power Supply Failed (single PSU failure)
5. Fan Failure
6. Temperature Exceeds Threshold

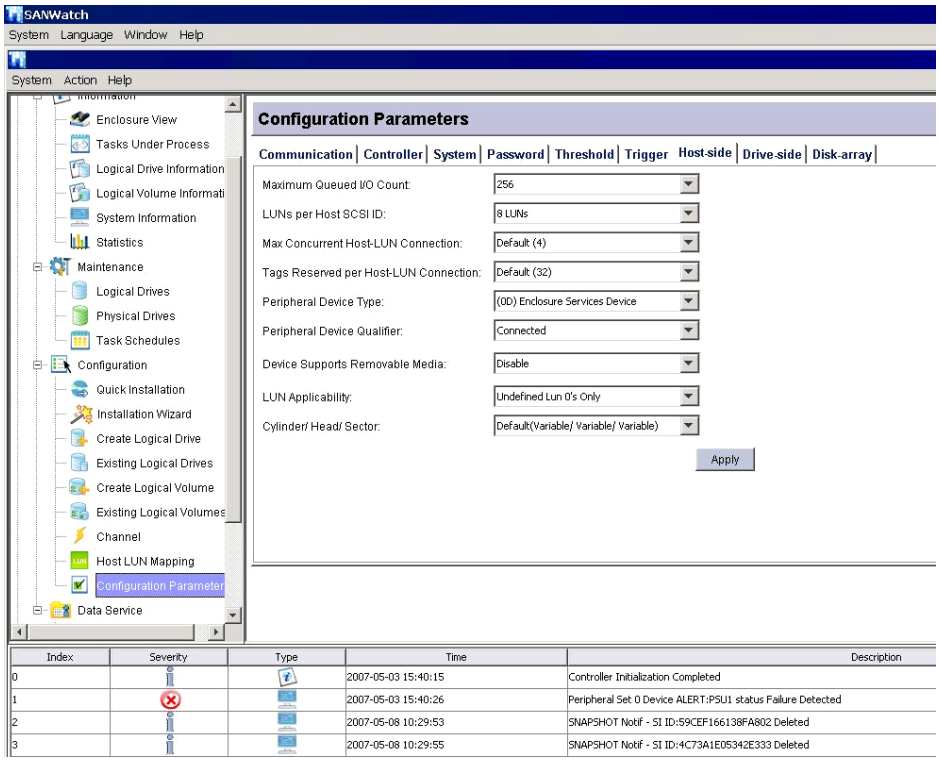
Each option is executed by a two-step procedure. Select the check box of the event type for which you wish the controller/subsystem to commence the cache flush, and then click **Apply** for the configuration to take effect.

NOTE:

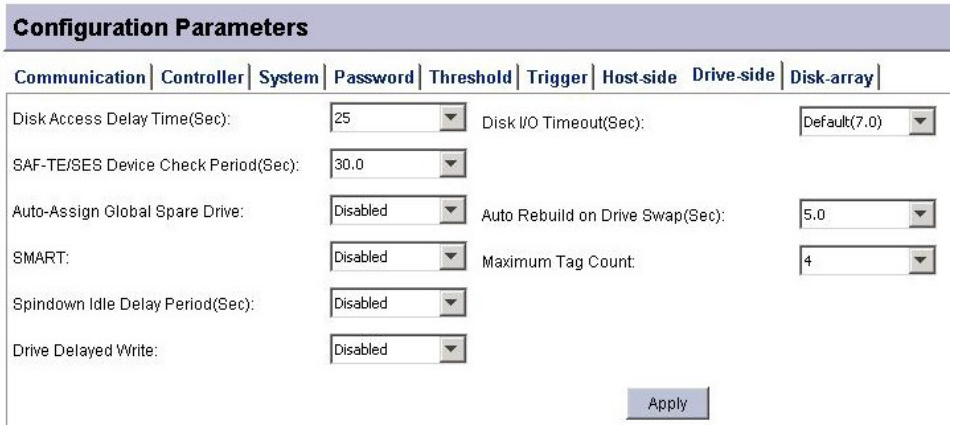
The thresholds on temperatures refer to the defaults set for "RAID controller board temperature."

7.9 Host-side, Drive-side, and Disk Array Parameters

I/O channel host-side, drive-side, and rebuild priority options are included in its specific sub-window. To configure these configuration options, select each configuration page from the Configuration Parameters window.


SANWatch
System Language Window Help
System Action Help
Enclosure View
Tasks Under Process
Logical Drive Information
Logical Volume Informati
System Information
Statistics
Maintenance
Logical Drives
Physical Drives
Task Schedules
Configuration
Quick Installation
Installation Wizard
Create Logical Drive
Existing Logical Drives
Create Logical Volume
Existing Logical Volumes
Channel
Host LUN Mapping
Configuration Parameter
Data Service
Configuration Parameters
Communication | Controller | System | Password | Threshold | Trigger | Host-side | Drive-side | Disk-array
Maximum Queued I/O Count: 256
LUNs per Host SCSI ID: 8 LUNs
Max Concurrent Host-LUN Connection: Default (4)
Tags Reserved per Host-LUN Connection: Default (32)
Peripheral Device Type: (0D) Enclosure Services Device
Peripheral Device Qualifier: Connected
Device Supports Removable Media: Disable
LUN Applicability: Undefined Lun 0's Only
Cylinder/ Head/ Sector: Default(Variable/ Variable/ Variable)
Apply
Index Severity Type Time Description
0 2007-05-03 15:40:15 Controller Initialization Completed
1 2007-05-03 15:40:26 Peripheral Set 0 Device ALERT:PSU1 status Failure Detected
2 2007-05-08 10:29:53 SNAPSHOT Notif - SI ID:59CEF166138FA802 Deleted
3 2007-05-08 10:29:55 SNAPSHOT Notif - SI ID:4C73A1E05342E333 Deleted

Each option is executed by a two-step procedure. Click to select a desired value from the pull-down menu, and then click **Apply** for the configuration to take effect. Some configuration changes may only take effect after resetting the subsystem.


Configuration Parameters
Communication | Controller | System | Password | Threshold | Trigger | Host-side | Drive-side | Disk-array
Disk Access Delay Time(Sec): 25
Disk I/O Timeout(Sec): Default(7.0)
SAF-TE/SES Device Check Period(Sec): 30.0
Auto-Assign Global Spare Drive: Disabled
Auto Rebuild on Drive Swap(Sec): 5.0
SMART: Disabled
Maximum Tag Count: 4
Spindown Idle Delay Period(Sec): Disabled
Drive Delayed Write: Disabled
Apply

Drive-side Parameters

- **Disk Access Delay Time (Sec)**: Sets the delay time before the subsystem tries to access the hard drives after power-on. Default can vary in different RAID subsystems.

- **Drive Check Period (Sec)**: This is the time interval for the controller to check all disk drives that were on the drive buses at controller startup. The default value is "Disabled." Disabled means that if a

drive is removed from the bus, the controller will not know it is missing as long as no host accesses that drive. Changing the check time to any other value allows the controller to check all array hard drives at the selected time interval. If any drive is then removed, the controller will be able to know – even if no host accesses that drive.

This option may not appear with drive channels that come with auto-detection, e.g., Fibre Channel.

- **Auto-assign Global Spare Drive:** Enable this function to allow the system to auto-assign one or more unused drives as the Global Spare drives. This can prevent the lack of spare drive when a spare has previously been spent rebuilding a logical drive, and yet a user forgets to configure another spare.

- **SMART:** This allows you to configure SMART-related functionality. SMART is short for "**Self-Monitoring, Analysis and Reporting Technology**." Options provided in the pull-down menu are the actions to be taken if the SMART function detects an unstable drive.

- **Spindown Idle Delay Period (Sec):** Subsystem firmware stops supplying 12V power source to hard drives when hard drives have not received I/Os for a period of time. When enabled, this feature helps reduce power consumption.

- **Drive Delayed Write:** This option applies to SATA disk drives which may come with embedded buffers. When enabled, write performance may improve. **However, this option should be disabled for mission-critical applications**. In the event of power outage or drive failures, data cached in drive buffers may be lost, and data inconsistency will occur. The default setting is "Disabled."

NOTE:

This function is only applicable on RAID subsystems running Firmware 3.47 or above using SATA hard drives.

- **Disk I/O Timeout (Sec):** This is the time interval for the subsystem to wait for a drive to respond to I/O requests. Selectable intervals range from 1 to 10 seconds.

- **SAF-TE/SES Device Check Period (Sec):** If enclosure devices in your RAID enclosure are being monitored via SAF-TE/SES enclosure service, use this function to decide at what interval the subsystem will check the status of these devices.

- **Auto Rebuild on Drive Swap (Sec)**: The subsystem scans drive buses at this interval to check if a failed drive has been replaced. Once a failed drive is replaced, firmware automatically commence a

rebuild on the logical drive. The Default drive bus check time is 1 second, which is different from this option, Auto Rebuild check time.

- **Maximum Tag Count:** The subsystem supports tag command queuing with an adjustable maximum tag count from 1 to 128. The default setting is "Enabled" with a maximum tag count of 32.

Host-side Parameters

- **Maximum Queued I/O Count:** This is the arrangement of the controller internal resources for use with a number of the current host nexus. It is a "concurrent" nexus, so when the cache is cleared up, it will accept a different nexus again. Many I/Os can be accessed via the same nexus.

  This function allows you to configure the maximum number of I/O queues the controller can accept from the host computer.

- **LUNs per Host ID:** Each SCSI ID can have up to 32 LUNs (Logical Unit Numbers). A logical configuration of array capacity can be presented through one of the LUNs under each host channel ID. Most SCSI host adapters treat a LUN like another SCSI device.

- **Max. Concurrent Host-LUN:** The configuration option adjusts the internal resources for use with a number of current host nexus. If there are four host computers (A, B, C, and D) accessing the array through four host IDs/LUNs (ID 0, 1, 2 and 3), host A through ID 0 (one nexus), host B through ID 1 (one nexus), host C through ID 2 (one nexus) and host D through ID 3 (one nexus) - all queued in the cache - that is called 4 nexus. If there are I/Os in the cache through four different nexus, and another host I/O comes down with a nexus different than the four in the cache (for example, host A access ID 3), the controller will return "busy." Note that it is "concurrent" nexus; if the cache is cleared up, it will accept four different nexus again. Many I/Os can be accessed via the same nexus.

- **Tag Reserved Per Host-LUN Connection:** Each nexus has 32 (the default setting) tags reserved. When the host computer sends 8 I/O tags to the controller, and the controller is too busy to process them all, the host might start to send less than 8 tags during every certain period of time since then. This setting ensures that the controller will accept at least 32 tags per nexus. The controller will be able to accept more than that as long as the controller internal resources allow - if the controller does not have enough resources, at least 32 tags can be accepted per nexus.

- **Peripheral Device Type / Peripheral Device Qualifier / Device Supports Removable Media / LUN applicability:** If no logical drive has been created and mapped to a host LUN, and the RAID

controller is the only device connected to the host SCSI card, usually the operating system will not load the driver for the host adapter. If the driver is not loaded, the host computer will not be able to use the in-band utility to communicate with the RAID controller. This is often the case when users want to start configuring a RAID using management software from the host. It will be necessary to configure the "**Peripheral Device Type**" setting for the host to communicate with the controller. If the "**LUN-0's only**" is selected; only LUN-0 of the host ID will appear as a device with the user-defined peripheral device type. If "**all undefined LUNs**" is selected, each LUN in that host ID will appear as a device with the user-defined peripheral device type.

For connection without a pre-configured logical unit and Ethernet link to a host, the in-band SCSI protocol can be used in order for the host to "see" the RAID subsystem. Please refer to the reference table below. You will need to make adjustments in those pull-down menus: Peripheral Device Type, Peripheral Device Qualifier, Device Support for Removable Media, and LUN Application.

Operation System	Peripheral Device Type	Peripheral Device Qualifier	Device Support for Removable Media	LUN Applicability
Windows 2000/2003	0xd	Connected	Either is okay	LUN-0's
Solaris™ 8/9 (x86 and SPARC)	0xd	Connected	Either is okay	LUN-0's
Linux RedHat 8/9; SuSE 8/9	0xd	Connected	Either is okay	LUN-0's

Table 7-1: Peripheral Device Type Parameters

Device Type	Settings
Enclosure Service Device	0xd
No Device Present	0x7f
Direct Access Device	0
Sequential-access Device	1
Processor Device	3
CD-ROM Device	5
Scanner Device	6
MO Device	7
Storage Array Controller Device	0xC
Enclosure Services Device	0xD

Unknown Device	0x1f

Table 7-2: Peripheral Device Type Settings

- **Cylinder/Head/Sector:** Drive capacity is decided by the number of blocks. For some operating systems (Sun Solaris, for example) the capacity of a drive is determined by the cylinder/head/sector count. For Sun Solaris, the cylinder cannot exceed 65535; choose "cylinder<65535," then the controller will automatically adjust the head/sector count for your OS to read the correct drive capacity. Please refer to the related documents provided with your operating system for more information.

  Cylinder, Head, and Sector counts are selectable from the configuration menus shown below. To avoid any difficulties with a Sun Solaris configuration, the values listed below can be applied.

Capacity	Cylinder	Head	Sector
<64 GB	Variable	64	32
64 - 128 GB	Variable	64	64
128 - 256 GB	Variable	127	64
256 - 512 GB	Variable	127	127
512 - 1 TB	Variable	255	127

Table 7-3: Cylinder/Head/Sector Mapping under Sun Solaris

Older Solaris versions do not support drive capacities larger than 1 terabyte. Solaris 10 now supports array capacity larger than 1TB. Set the values to the values listed in the table below:

Capacity	Cylinder	Head	Sector
> 1 TB	< 65536	255	Variable
		Variable	255

Table 7-4: Cylinder/Head/Sector Mapping under Sun Solaris

The values shown above are for reference only and may not apply to all applications.

- **Login Authentication with CHAP:** This option allows you to enable or disable the login authentication with the Challenge Handshake Authentication Protocol (CHAP) function. CHAP enables the username and password to be encrypted against eavesdroppers.

  Both One-way and Two-way (Mutual) CHAP approaches are available through the "iSCSI Initiator" menu under the "Host LUN mapping" window.

NOTE:

- The CHAP configuration option here enables CHAP configuration menu in the host LUN mapping window.
- Unlike previous SANWatch and firmware revisions, controller name and password are no longer used for CHAP authentication.

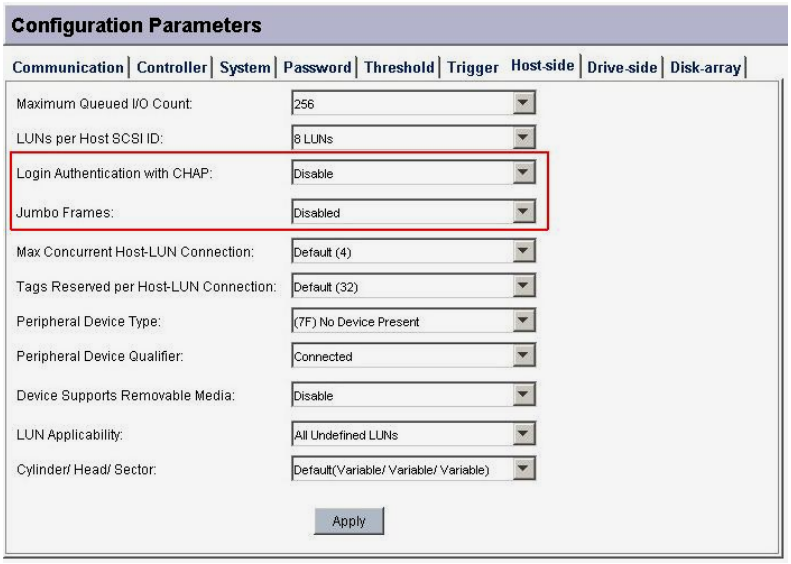


Figure 7-1: The Host-side Parameters Page for iSCSI Models

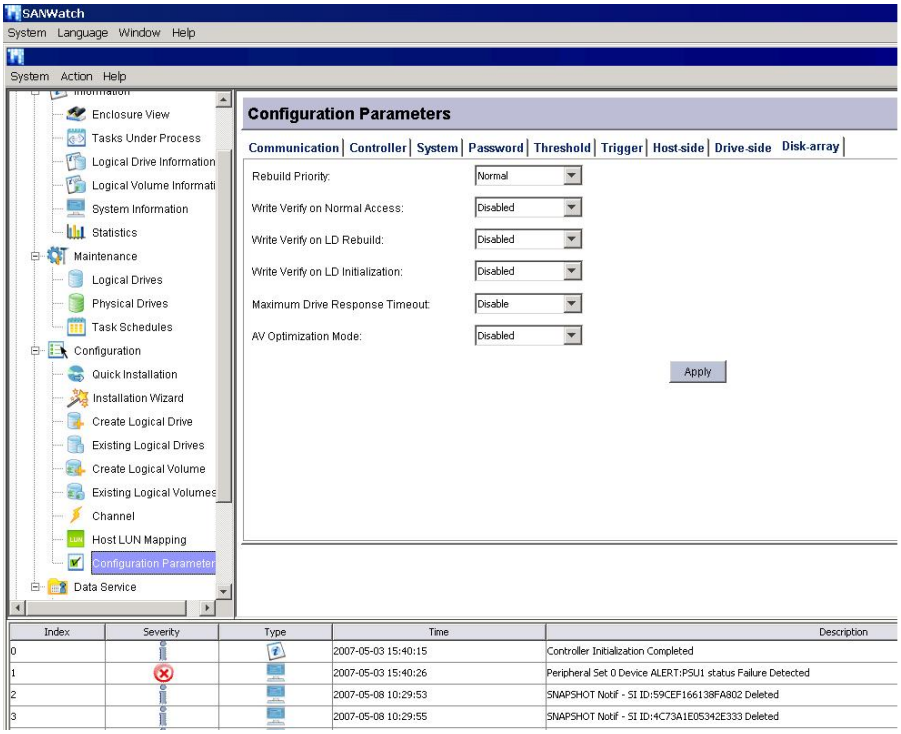
- **Jumbo Frames:** Jumbo Frames, as specified by the IEEE 802.3 standard, improve network performance for more data can be transmitted in one frame reducing interrupt load.

  The system default for this option is "disabled." If you want to enable this option, reset the subsystem for the configuration change to take effect.

CAUTION!

- The default and supported frame size is 9014 bytes. All devices on the network path must be configured with the same jumbo frame size.
- Configuration changes must be made in the Network Interface Card (NIC), through the configuration interface and tools provided by the NIC manufacturer. Check with your manufacturer to verify that this feature is supported. The network equipment (Ethernet switches, routers, and so forth) between the host and the subsystem must also be configured to accept Jumbo frames.

Disk-Array Parameters



- **Rebuild Priority:** The rebuild priority determines how much of the system resources are applied when rebuilding a logical drive. Available options are Low, Normal, Improved, and High. The higher priority takes up more system resources and the rebuild process completes more rapidly. However, I/O performance in the meantime is inevitably lower due to the resources consumed.

- **Write-Verify Options:** Errors may occur when a hard drive writes data. In order to avoid write errors, the controller can force the hard drives to verify the written data. There are three selectable methods:

  1. **Verification on LD Normal Access:**

     Performs Verify-after-Write during normal I/O requests.

  2. **Verification on LD Rebuild Writes:**

     Performs Verify-after-Write during the rebuilding process.

  3. **Verification on LD Initialization Writes:**

     Performs Verify-after-Write while initializing the logical drive.

- **Maximum Drive Response Timeout (ms):** The main purpose for having a maximum response time on hard drives is to ensure delays caused by media errors or drive erratic behaviors do not result in host

I/O timeouts. Doing so can avoid the unnecessary efforts dealing with delays especially when drives showing problems are often the failing drives. Below are some operation limitations:

- Battery shall be present and functioning properly.
- Write-Back policy is enabled.
- Only available for RAID level 1, 3, 5 and 6.

Failures of a hard drive to return I/Os before the Response Timeout will force the firmware to retrieve requested I/Os from the other members of the logical drive.

NOTE:

This function is only applicable on RAID subsystems running Firmware 3.42 or above version.

- **AV Optimization Mode:** The AV optimization is applied for the emerging Audio/Video or non-drop frame applications such as the VOD/MOD, NLE (Non-Linear Editing), and multi-streaming environments.

  Fewer Steams: (for applications featuring sequential I/Os and large block sizes; e.g., Video Editing)

  1. The Maximum Drive Response Timeout will be automatically set to 160ms.
  2. The drive cache-flush threshold is set to a value lower than Infortrend's traditional Write-back Flush threshold.
  3. A minimum read-ahead size is determined by the Stripe size.
  4. Enhance performance using LMDD test in the sequential reads.
  5. The Synchronized Cache Communications between RAID controllers is disabled.

  Multiple Steams: (for applications featuring smaller I/Os and more outstanding I/Os, e.g., Media Broadcasting)

  1. The Maximum Drive Response Timeout will be automatically set to 960ms.
  2. The Write-back Flush threshold is set to a value lower than Infortrend's traditional Write-back Flush threshold.
  3. Enhance performance using LMDD test in the sequential reads.

4. The Synchronized Cache Communications between RAID controllers is disabled.

NOTE:

Some parameters related to AV Optimization will be implemented as system defaults in the append file for specific ODM/OEM models.

Chapter 8

Channel Configuration

Using SANWatch Manager, you can modify the configuration of any channel on the controller. You can set the channel operation mode to host or drive, enable or disable channel termination, add/delete channel IDs, set the transfer clock rate for synchronous communications, and select the transfer width.

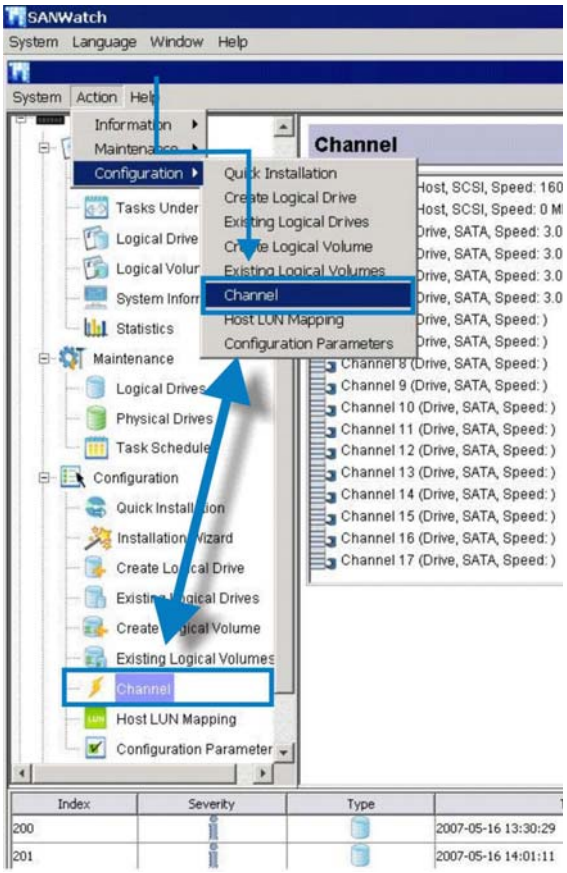
Channel configuration settings are available under the **Physical View** in the RAID View window. This chapter describes the following Channel Configuration features:

- **Channel Configuration Window – Section 8.1, page 8-2**
- **User-Configurable Channel Parameters – Section 8.2, page 8-3**
  - **8.2.1 Channel Mode**
  - **8.2.2 Termination**
  - **8.2.3 Default Transfer Clock (in MHz)**
  - **8.2.4 ID Pool / AID / BID**
- **Setting the Configurations for a Channel - Section 8.3, page 8-7**

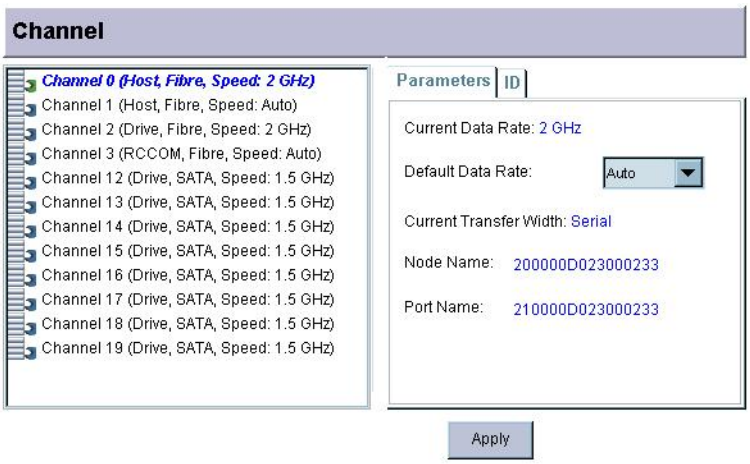
8.1 Channel Configuration Window

I/O Channel configuration options are available under the **Configuration** category, which is found in the lower section of the navigation panel.

To access the **Channel** window, use either the command from the Action menu or select the **Channel** icon from the navigation panel.



Once the **Channel** window has been opened and channel items have appeared, click on the channel that needs to be configured and its configuration window will appear on the right.


Channel
Channel 0 (Host, Fibre, Speed: 2 GHz)
Channel 1 (Host, Fibre, Speed: Auto)
Channel 2 (Drive, Fibre, Speed: 2 GHz)
Channel 3 (RCCOM, Fibre, Speed: Auto)
Channel 12 (Drive, SATA, Speed: 1.5 GHz)
Channel 13 (Drive, SATA, Speed: 1.5 GHz)
Channel 14 (Drive, SATA, Speed: 1.5 GHz)
Channel 15 (Drive, SATA, Speed: 1.5 GHz)
Channel 16 (Drive, SATA, Speed: 1.5 GHz)
Channel 17 (Drive, SATA, Speed: 1.5 GHz)
Channel 18 (Drive, SATA, Speed: 1.5 GHz)
Channel 19 (Drive, SATA, Speed: 1.5 GHz)
Parameters
ID
Current Data Rate: 2 GHz
Default Data Rate:
Auto
Current Transfer Width: Serial
Node Name: 200000D023000233
Port Name: 210000D023000233
Apply

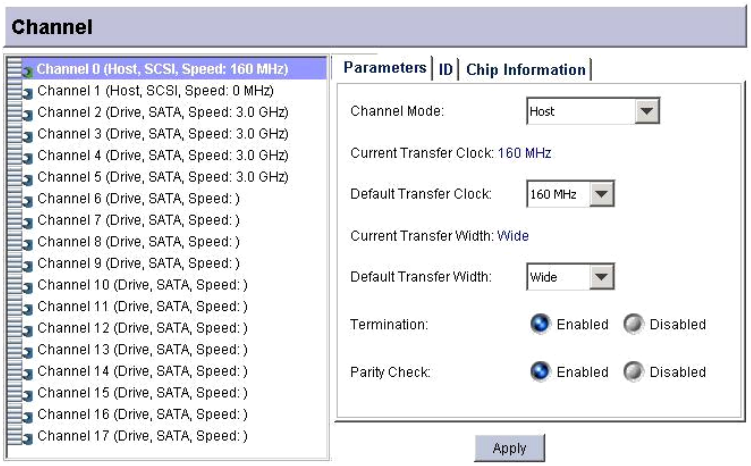
The following sections describe user-configurable channel parameters.

8.2 User-Configurable Channel Parameters

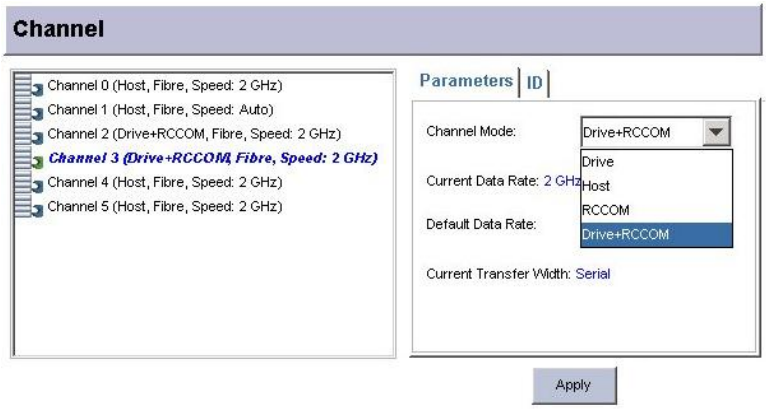
Once the channel has been selected, the screen shown in *Error! Reference source not found.* will appear in the content window. The different options are discussed below.

A SCSI host channel is shown below:

Channel Parameters: EonStor Series


Channel
Channel 0 (Host, SCSI, Speed: 160 MHz)
Channel 1 (Host, SCSI, Speed: 0 MHz)
Channel 2 (Drive, SATA, Speed: 3.0 GHz)
Channel 3 (Drive, SATA, Speed: 3.0 GHz)
Channel 4 (Drive, SATA, Speed: 3.0 GHz)
Channel 5 (Drive, SATA, Speed: 3.0 GHz)
Channel 6 (Drive, SATA, Speed:)
Channel 7 (Drive, SATA, Speed:)
Channel 8 (Drive, SATA, Speed:)
Channel 9 (Drive, SATA, Speed:)
Channel 10 (Drive, SATA, Speed:)
Channel 11 (Drive, SATA, Speed:)
Channel 12 (Drive, SATA, Speed:)
Channel 13 (Drive, SATA, Speed:)
Channel 14 (Drive, SATA, Speed:)
Channel 15 (Drive, SATA, Speed:)
Channel 16 (Drive, SATA, Speed:)
Channel 17 (Drive, SATA, Speed:)
Parameters
ID
Chip Information
Channel Mode:
Host
Current Transfer Clock: 160 MHz
Default Transfer Clock:
160 MHz
Current Transfer Width: Wide
Default Transfer Width:
Wide
Termination:
Enabled
Disabled
Parity Check:
Enabled
Disabled
Apply

Channel Parameters: EonStor 1U Controller Head Series



8.2.1. Channel Mode

This configuration option is exclusively available with the EonStor 2510FS controller head and Fibre-to-Fibre RAID subsystems.

The EonStor series controller allows flexible reconfigurations of its I/O channels. An I/O channel can be assigned as **Host**, **Drive**, dedicated **RCC** (**RCCOM**), or **Drive+RCCOM** channels. For example, the combination of I/O channels may look like the following:

Dual-Redundant Controller Models	
EonStor 2510FS-4RH	2 hosts and 2 drive+RCCOMs; a total of 4 I/O channels
EonStor 2510FS-6RH	2 hosts, 2 dedicated RCCOMs, and 2 drives; a total of 6 I/O channels

Table 8-1: Dual-Redundant Controller Channel Modes

Dual-Single Controller Models	
EonStor 2510FS-4D	2 hosts and 2 drives per controller; a total of 8 I/O channels
EonStor 2510FS-6D	2 hosts and 4 drives or 4 hosts and 2 drives per controller; a total of 12 I/O channels

Table 8-2: Dual-Single Controller Channel Modes

For more information about all possible combinations, please refer to the ***Installation and Hardware Reference Manual*** that came with your controller.

For the latest ASIC400 series, there are preset, dedicated SATA channels for RCC communications and there is no need to configure specific host/drive channels for RCC communications.

8.2.2. Termination

This parameter enables or disables channel SCSI termination on subsystems featuring SCSI host channels. SCSI buses must be properly terminated at both ends; that is, when connecting one end of a SCSI cable to a host HBA, the termination of the channel must be enabled on the subsystem side. An alternate configuration should be applied when multiple enclosures are cascaded on the host buses. An enclosure situated in the middle of a SCSI bus should have its termination set to disabled.

IMPORTANT!

Some later SCSI RAID models have a sense pin on their SCSI ports that activates SCSI bus termination if the subsystem is the end device on a SCSI bus. The firmware default for SCSI bus termination is enabled, which also enables the auto-sensing mechanism. You may use external SCSI terminators, but you do not have to disable SCSI termination of systems between the end devices using firmware or the SANWatch software.

8.2.3. Default Transfer Clock (in MHz)

These parameters set the data transfer clock rate for synchronous communication over the SCSI bus, and enable or disable wide transfer, respectively.

Data transferred across the bus in synchronous transfer mode is clocked using a synchronous transfer clock signal. The frequency of this signal determines the rate at which data is transferred. For example, if the synchronous transfer clock is 10 MHz, data transfer rate will be 10 million bytes per second (using narrow transfer).

Data transfer across the SCSI bus can be either 8-bits or 16-bits at a time. The former is referred to as *narrow* transfer, while the latter is referred to as *wide* transfer. According to SCSI channel specifications, transfer speed shown in MHz is the SCSI bus synchronous frequency. At the same synchronous transfer clock rate, 16-bit wide transfer rate is double of 8-bit narrow transfer rate. Please refer to the transfer speed in the table below.

Transfer Rate	Clock Speed in MHz
SCSI-320	160MHz
SCSI-160	80MHz

Table 8-3: SCSI Channels Clock Speeds

NOTE:

Infortrend's SCSI products are backward compatible with older version of SCSI type. However, using older versions of SCSI type may slow down the data transferring speed and you may not be able to enjoy some of the new SCSI features.

Under conditions in which SCSI signal quality is poor, such as with extremely long cables, poor connections, or bad termination, it may occasionally be necessary to reduce the synchronous transfer clock to allow the SCSI channel to function normally.

Furthermore, certain older SCSI devices may only support *narrow* transfer and behave abnormally when attempting to negotiate *wide* transfer. Under such conditions, *wide* transfer may need to be disabled, forcing the controller to use *narrow* transfer mode with that device.

IMPORTANT!

Every time you change the transfer speed, you must reset the controller for the changes to take effect.

8.2.4. ID Pool / AID / BID

The selection with AID (Slot A controller ID) and BID (Slot B controller ID) only appears with controller/subsystems that come with dual-redundant RAID controllers.

This parameter sets the IDs to appear on the host channels. Each channel must have a unique ID in order to work properly. For a SCSI-host subsystem, IDs range from 0 to 15. For an iSCSI-host subsystem, IDs range from 0 to 3. For a Fibre-host controller/subsystem, IDs range from 0 to 125. ID 0 is the default value assigned for host channels on SCSI-host and iSCSI-host subsystems and ID 112/113 is the default value assigned for host channels on Fibre-host controller/subsystems. Preset IDs are available with drive channels and it is recommended to keep the defaults.

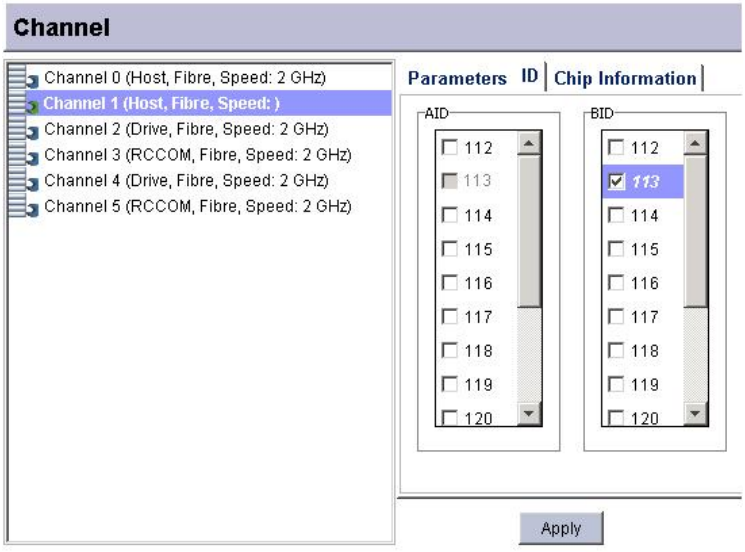
For more information on host channel and drive channel IDs, please refer to the ***Operation Manual*** and the hardware documentation that came with your controller/subsystems.

8.3 Setting the Configurations for a Channel

Step 1. Single-click under the **Channel** window to select a corresponding channel. Channel icons are displayed in the left-side panel of the configuration window. The Channel Settings configuration will appear as two separate pages on the right side: **Parameters** and **ID**.

Step 2. From the **Parameters** panel, specify a preferred value with configurable items either by checking the pull-down menus or radio buttons of the **transfer clock**, **transfer width**, **termination**, and/or **parity check**. Be sure to click the **Apply** button for the changes to take effect.

Step 3. If you want to assign a different ID to the selected channel, choose the **ID** panel. An **ID pool** scroll menu will appear as shown below.



When selecting an ID, be sure that it does not conflict with the other devices on the channel. Preset IDs should have been grayed out and excluded from selection. IDs assigned to an alternate RAID controller will also be excluded. The ID pool lists all available IDs for the current selection. Highlight the IDs you want to use by selecting their check boxes and click **Apply** to create either the **AIDs** (Slot A controller ID, which is the default Primary controller) or **BIDs** (Slot B controller ID) for the channel.

A system reset is necessary for the configuration change to take effect.

This page is intentionally left blank.

Chapter 9
Drive Management

This chapter focuses on how to create or delete Logical Drives (LDs) and Logical Volumes (LVs). Both LDs and LVs can be partitioned. This chapter describes the following drive management features:

- **Locating Drives – Section 9.1, page 9-3**
- **Logical Drive Management – Section 9.2, page 9-3**
  - **Accessing the Create Logical Drive** Window
  - **9.2.2 Creating Logical Drives**
    - **9.2.2.1 Logical Drive** Creation
    - **9.2.2.2 Selecting Drives**
    - **9.2.2.3 Setting RAID Parameters**
    - **9.2.2.4 Click OK to Create an** LD
  - **9.2.3 Accessing the Existing Logical Drive Window**
    - **9.2.3.1 Modifying LD Configurations**
    - **9.2.3.2 Expanding LD by Adding Disks**
    - **9.2.3.3 Accessing the Expand Command**
    - **9.2.3.4 Click Expand to Initiate LD**
    - **9.2.3.5 Accessing the Migrate LD Command page**
    - **9.2.3.6 Migration**
  - **9.2.4 Dynamic Logical Drive Expansion**
    - **9.2.4.1 What Is It and How Does It Work?**
    - **9.2.4.2 Two Expansion Modes**

- **9.2.5 Adding Spare Drives**
  - **9.2.5.1 Accessing the Spare Drive Management Screen**
- **Rebuilding Logical Drives**
- **9.2.7 Deleting an LD**

♦ **Logical Volume Management – Section 9.3, page 9-20**

- **Accessing the Create Logical Volume Window**
- **Creating Logical** Volumes
  - **9.3.2.1 LV Creation**
  - **9.3.2.2 Selecting LDs**
  - **9.3.2.3 Setting Logical Volume** Parameters
  - **9.3.2.4 Click OK to Create**
- **9.3.3 Accessing the Existing Logical Volume**
  - **9.3.2.2 Expanding a Logical** V
  - **9.3.3.3 Accessing the Expand Logical Volume Page**
- **9.3.4 Deleting a Logical** V

♦ **Partitioning a Logical Configuration – Section 9.4, page 9- 27**

- **9.4.1 Overview**
- **9.4.2 Partitioning a Logical Drive**
- **9.4.3 Partitioning a Logical Volume**

♦ **Physical Drives Maintenance – page 9-31**

- **9.5.1 Read/Write Test**

9.1. Locating Drives

SANWatch uses icons to represent subsystem drive trays. In many configuration windows, a single click on a drive tray icon selects a hard drive. Drive status is indicated and automatically refreshed by displaying icons of different colors. The drive tray icons used in the **Front View** window to instantly display drive status are shown below. By referring to the drive status in the **Front View** window, you can start to create or configure a logical array.

Drive Conditions	Graphical Identification
New or healthy **Used** drive	
Bad or **Missing** drive	
Spare Drive (Local/Global/Enclosure)	

Before you start configuring a logical array, please read the following:

- All members in a logical configuration are displayed in the same unique color.
- Whenever a disk drive is selected by a single mouse click on its icon, the drive's status is displayed on the associated configuration window. For example, when a drive is selected by a single mouse click, it automatically appears in the Selected Members column. In this way, mistakes can be avoided by double-checking the information related to a specific disk drive.

9.2. Logical Drive Management

This section describes how to:

- Access the **Logical Drive (LD) Creation and Management** Windows
- Create LDs
- Expand LDs
- Migrate LDs
- Delete LDs

NOTE:

When you delete a logical drive, all physical drives assigned to the logical drive will be released, making them available for regroup or other uses.

9.2.1 Accessing the Create Logical Drive Window

LDs are created in the **Create Logical Drive** window and managed in the **Existing Logical Drives** window. These functional windows are accessed from the command from the Action menu or SANWatch's navigation panel on the left of the GUI screen.

Step 1. To manage LDs, such as to create and set related parameters, display the **Create Logical Drive** window by clicking on the **Create Logical Drive** icon in the functional navigation panel or clicking on the **Action** menu items located on top of the screen.

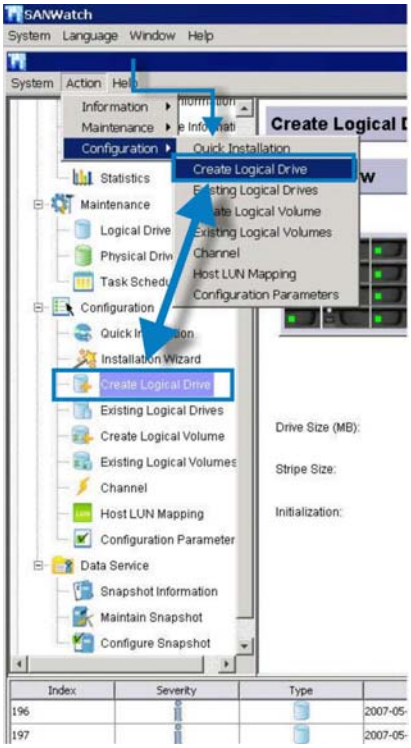
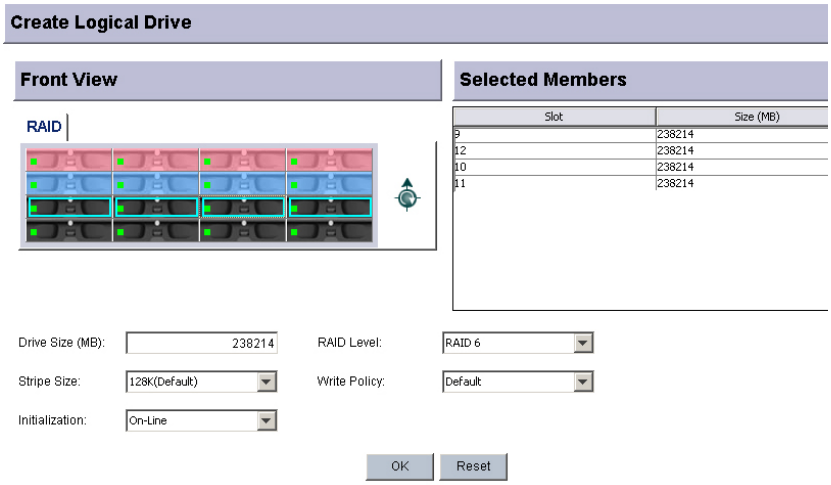


Figure 9-1: Access to the Create Logical Drive Window

Step 2. The configuration screen as shown below will appear.



9.2.2 Creating Logical Drives

9.2.2.1. Logical Drive Creation Process

To create a logical drive:

Step 1. Select the physical drives that will be included in the LD. (See ***Section 9.2.2.2***)

Step 2. Select the following RAID array parameters. (See ***Section 9.2.2.3***)

- Drive Size (the maximum drive capacity used in each member drive – often the size of the smallest member)
- Stripe Size
- Initialization Mode
- RAID Level
- Write Policy

Step 3. Click the **OK** button. (See ***Section 9.2.2.4***) The **Reset** button allows you to cancel previous selections.

9.2.2.2. Selecting Drives

Step 1. Select members for the new logical drive by clicking drive icons in the **Front View** window. Bad drives or drives belonging to another logical drive will not be available for the mouse-click selection.

Step 2. Disk drives selected for a new logical drive will be listed in the **Selected Members** sub-window on the right-hand side of the screen.

Step 3. Continue to set appropriate RAID parameters using the dropdown lists at the lower half of the configuration screen.

9.2.2.3. Setting RAID Parameters

Drive Size

The value entered in the ***Drive Size*** field determines how much capacity from each drive will be used in the logical drive. It is always preferred to include disk drives of the same capacity in a logical configuration.

NOTE:

Enter a smaller number if you do not want to use up all of the capacity at this time. This also applies if you suspect your disk drives may be featuring different block numbers. The unused capacity can be utilized later using the **Expand Logical Drive** function.

Selecting Stripe Size

The stripe size used when the LD is created can be selected from the **Stripe Size** pull-down menu. The stripe sizes ranging from 16K to 1024K are available. A default stripe size is available and is indicated by bracketed information.

Select a stripe size, but note that stripe size arrangement has a tremendous effect on RAID subsystem performance. Changing stripe size is only recommended for experienced users. Stripe size defaulted to this menu is determined by the subsystem Optimization mode and the RAID level selected.

Initialization Options

If set to the Online mode, you can have immediate access to the array. "Online" means the logical drive is immediately available for I/Os and the initialization process can be automatically completed in the background.

Select RAID Level

From the **RAID Level** pull-down menu shown, select the RAID level you wish to apply to the LD.

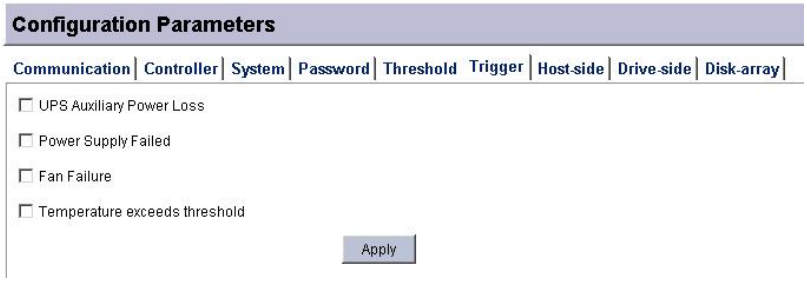
Write Policy

Define the write policy that will be applied to this array. "Default" is actually an option that is automatically coordinated with the subsystem's general setting. The general caching mode setting can be accessed through the **Controller** -> **Caching Parameters** section of the **Configuration Parameters** sub-window.

NOTE:

The **Default** option should be considered as "**Not-Specified**." If a logical drive's write policy is set to Default, the logical drive's caching behavior will be automatically controlled by firmware. In the event of component failure or violated temperature threshold, Write-back caching will be disabled and changed to a conservative "Write-through" mode.

When set to "Default," the caching mode will be automatically adjusted as part of the event triggered responses.


Configuration Parameters
Communication | Controller | System | Password | Threshold | Trigger | Host-side | Drive-side | Disk-array |
UPS Auxiliary Power Loss
Power Supply Failed
Fan Failure
Temperature exceeds threshold
Apply

9.2.2.4. Click OK to Create an LD

Step 1. Click the **OK** button.

Step 2. A confirm message will appear showing the LD is successfully created.

When the initialization process begins, you can check the **Tasks Under Process** window to view its progress.

9.2.3 Accessing the Existing Logical Drive Window

Various functions can be performed on configured arrays in the **Existing Logical Drives** window. The window is accessible from the **Action** menu or SANWatch's navigation panel on the GUI screen.

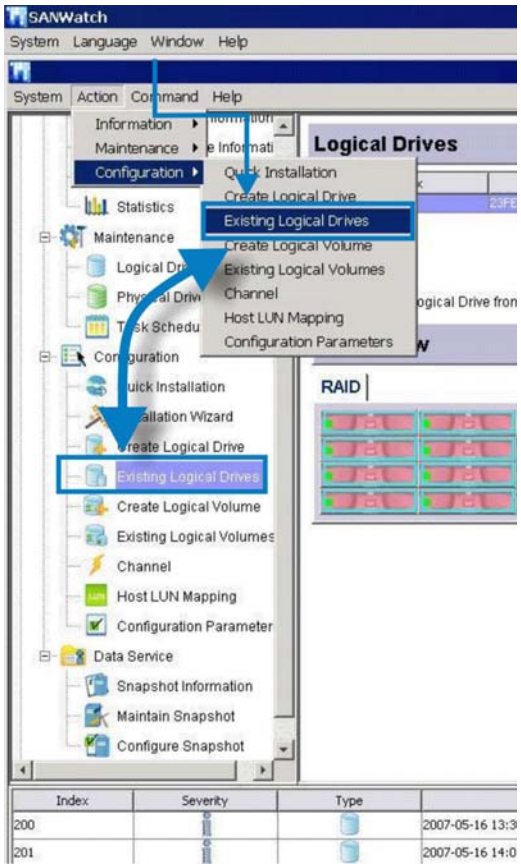
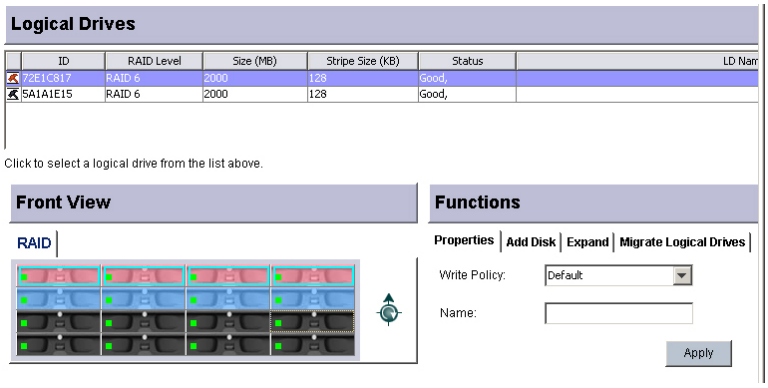


Figure 9-2: Accessing the Existing Logical Drives Window

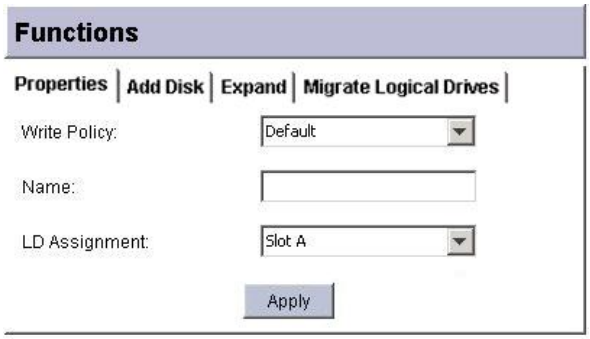
On the **Existing Logical Drives** window**,** the LDs that have previously been created appear in the **Logical Drives** panel.



From the list shown above**,** select the LD for which you wish to change its characteristics. Once selected, its members will be highlighted in the **Front View** sub-window. In the **Functions** window, several function tabs (e.g., **Properties**, **Add Disk, Expand**, etc.) will appear.

9.2.3.1. Modifying LD Configurations

After the LD is created, some configurations can be modified in the **Properties** command page. To access the page, select a logical drive and click on the **Properties** tab on the **Functions** window.



Each option is executed by a two-step procedure. Click to select a desired value from the pull-down menu or input a name, and then click **Apply** for the configuration to take effect.

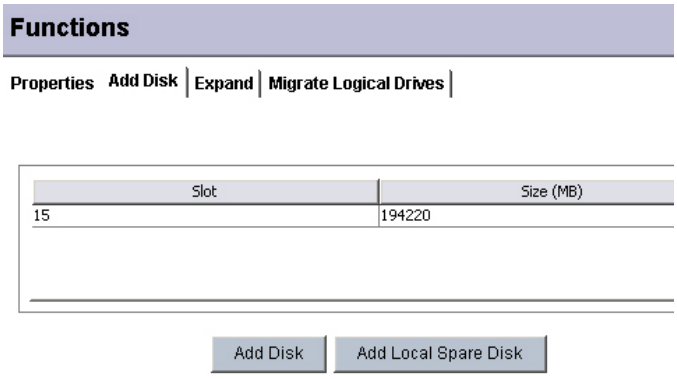
Write Policy: Write policy can be adjusted on a per logical drive basis. This option allows you to set a write policy for the specific logical drive you selected. "Default" is a neutral value that is coordinated with the controller's caching mode setting. Other choices are "Write-back" and "Write-through."

Name: You can name a logical drive per logical drive basis.

LD Assignment: both controllers can access a logical drive. In traditional LD management, one LD can only be accessed either by a primary or a secondary controller. In system running later firmware releases, LD assignment is referred to controller locations, Slot A or Slot controller.

9.2.3.2. Expanding LD by Adding Disks

To access the **Add Disk** command page, select a logical drive and click on the **Add Disk** tab under **Functions** window.



Step 1. Select the logical drive you wish to expand from the LD list on top of the GUI screen.

Step 2. Select the **Add Disk** tab to display the content panel.

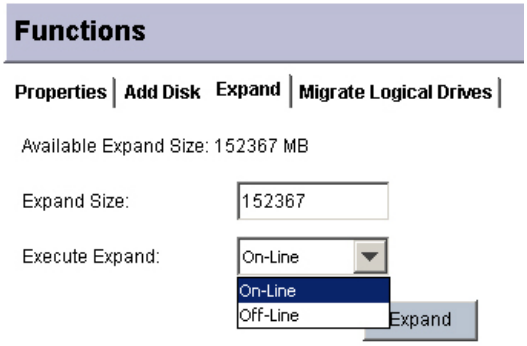
Step 3. Select one or more drives you wish to add to the logical drive by a single mouse-click from the **Front View** window. When a drive is selected, its status is displayed in the **Add Disk** content panel.

Step 4. The **Add Disk** panel has two functional buttons: **Add Disk** and **Add Local Spare Disk**. Click on the **Add Disk** button to include new members into the array.

Step 5. The **Add Disk** process should immediately begin. You may check the add drive progress in the **Tasks Under Process** window.

9.2.3.3. Accessing the Expand Command page

To access the **Expand** command page, select a logical drive and click on the **Expand** tab under the **Functions** window.



Available Expansion Size (MB)

If there is an amount of unused capacity in a logical drive, the LD can be expanded. If there is no amount present in the text box, then the LD cannot be expanded.

Set Expansion Size

A value can be entered in this text box if an amount is shown in the **Expand Size** text box. The value entered into the **Expansion Size** text box cannot exceed the amount shown in the text box above. The value entered here specifies the size of expansion capacity that will be added to the array.

Execute Expand

The **Execute Expand** list determines whether the expansion will be processed in an online or an offline manner. With an online expansion, the expansion process will begin once the subsystem finds I/O requests from the host become comparatively low. If an offline expansion is preferred, then the expansion process will immediately begin.

9.2.3.4. Click Expand to Initiate LD Expansion

To initiate the LD expansion, follow these steps:

Step 1. Once the LD expansion parameters have been selected, click the **Expand** button at the bottom of the **Expand** page.

Step 2. The expand process begins and you may check the progress in the **Tasks Under Process** window.

Step 3. The expansion capacity will appear as a new partition. You may right-click a logical drive listed above to display the **Edit Partition** command to verify the expansion size.

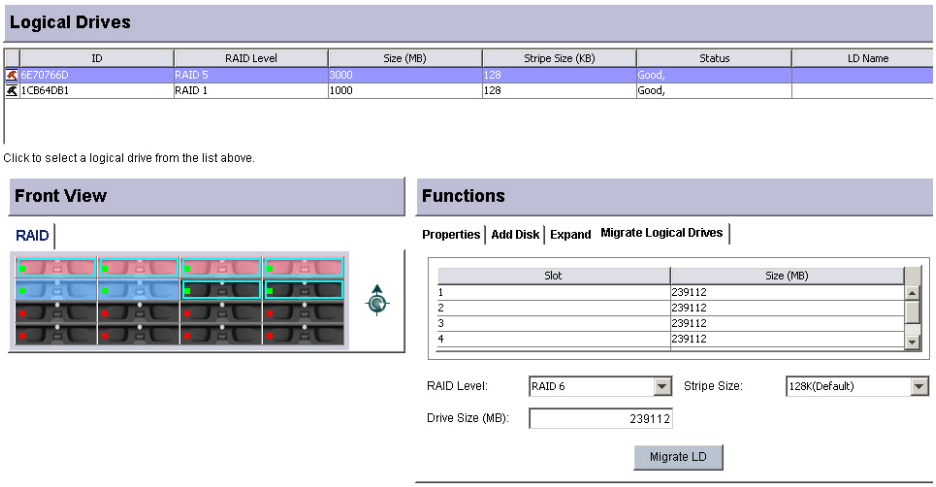
9.2.3.5. Accessing the Migrate LD Command page

To access the **Migrate LD** command page, first select a logical drive on the list and then click on the **Migrate Logical Drives** tab under the **Functions** window. (See ***Figure 9-8***)

NOTE:

Currently firmware only supports the migration between RAID levels 5 and 6. This function is disabled when an LD is configured in other RAID levels.

This function is only applicable on RAID subsystems running Firmware revision 3.47 or above.



Select a RAID Level

There are numerous RAID levels, each level is a different way to spread data across multiple disk drives. Selecting a RAID level that is most appropriate for your application with a balance among usable capacity, performance, and fault tolerance. Currently SANWatch supports RAID migration between RAID5 and RAID6. For more information about RAID levels, please refer to **Appendix C** of this manual.

You need a minimum of three (3) drives for RAID 5 and four (4) drives for RAID 6. The RAID level dropdown list displays applicable RAID levels according to your current selection. If you need to add a disk drive for more capacity, (for example, when migrating from RAID5 to RAID6) you can select an unused drive from the **Front View** window. A selected drive is displayed in the same color as the logical drive to which it will be added. To deselect a drive, click again on the selected drive. The slot number and drive size information will also be reflected accordingly through a drive list on the right.

Select a Stripe Size

Choose different stripe size may affect the performance of RAID subsystem. Base on the applications, users should choose a best-fit stripe size to achieve the best data transfer rate. The following stripe sizes are available: 16KB, 32KB, 64KB, 128KB, 256KB, 512KB, or 1024KB. A default stripe size is pre-selected.

Select a stripe size, but note that stripe size arrangement has a tremendous effect on RAID subsystem performance. Changing stripe size is only recommended for experienced users. Stripe size defaulted to this menu is determined by the subsystem Optimization mode and the RAID level selected.

Set a Drive Size

In the Drive Size (MB) input box displays the maximum drive size of the smallest member. Decreasing this value can create a smaller logical drive. The remainder can be used later by expanding the drive (as explained in ***Section 9.2.3.3.***)

9.2.3.6. Migration Process

To initiate the LD expansion, follow these steps:

Step 1. Once the LD migration parameters have been set to the desired values, click the **Migrate LD** button at the bottom of the **Migrate Logical Drives** page.

Step 2. The migration process begins and you may check the progress in the **Tasks Under Process** window.

9.2.4 Dynamic Logical Drive Expansion

9.2.4.1. What Is It and How Does It Work?

Before Dynamic Logical Drive Expansion, increasing the capacity of a RAID system using traditional methods meant backing up, re-creating, and then restoring data. Dynamic Logical Drive Expansion allows you to expand an existing logical array without powering down the system and without adding a storage enclosure.

9.2.4.2. Two Expansion Modes

There are two expansion modes.

Mode 1: Add Drive

Mode 1 Expansion is illustrated in ***Figure 9-3*** and involves adding more hard disk drives to a logical drive, which may require purchasing an enclosure with more drive bays. The data will be re-striped onto the original and newly added disks.

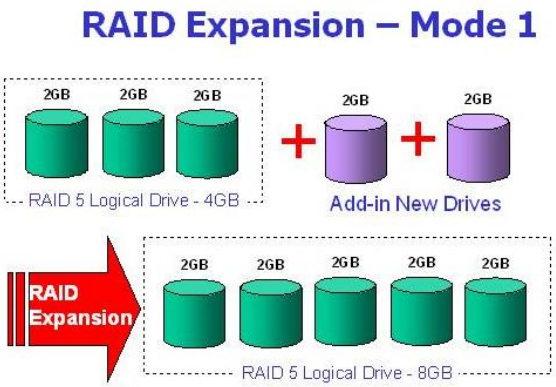


Figure 9-3: RAID Expansion Mode 1

As shown above, new drives are added to increase the capacity of a 4-Gigabyte (GB) RAID5 logical drive. The two new drives increase the capacity to 8GB.

Mode 2: Copy & Replace

Mode 2 Expansion requires each of the array members to be replaced by higher-capacity hard disk drives.

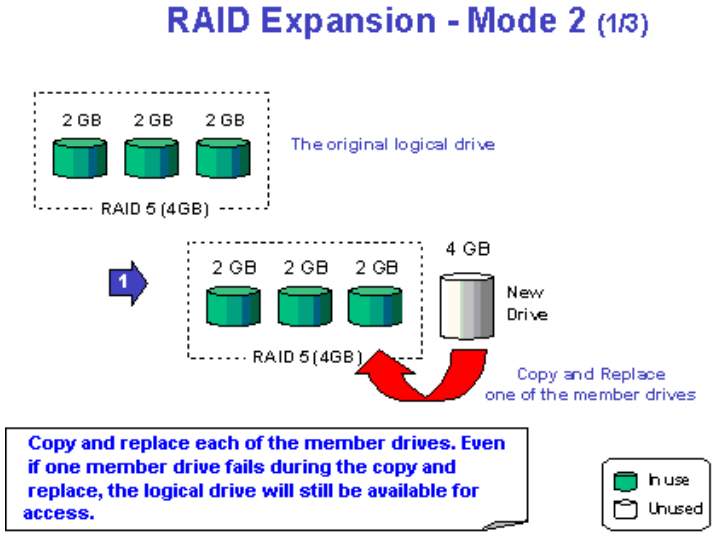

RAID Expansion - Mode 2 (1/3)
2 GB
2 GB
2 GB
The original logical drive
RAID 5 (4GB)
1
2 GB
2 GB
2 GB
4 GB
New Drive
RAID 5 (4GB)
Copy and Replace one of the member drives
Copy and replace each of the member drives. Even if one member drive fails during the copy and replace, the logical drive will still be available for access.
In use
Unused

Figure 9-4: RAID Expansion Mode 2 (1/3)

The diagram above illustrates expansion of the same 4GB RAID 5 logical drive using Mode 2 Expansion. Member drives are copied and replaced, one by one, onto three higher-capacity disk drives.

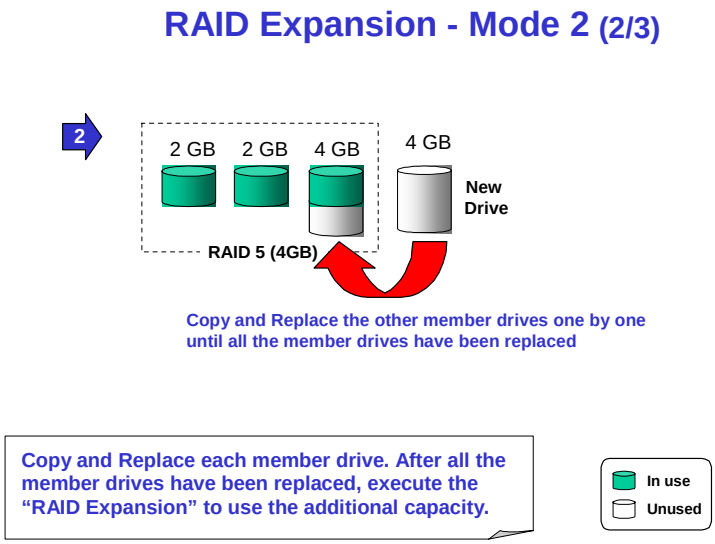

RAID Expansion - Mode 2 (2/3)
2
2 GB
2 GB
4 GB
4 GB
New Drive
RAID 5 (4GB)
Copy and Replace the other member drives one by one until all the member drives have been replaced
Copy and Replace each member drive. After all the member drives have been replaced, execute the "RAID Expansion" to use the additional capacity.
In use
Unused

Figure 9-5: RAID Expansion Mode 2 (2/3)

This results in a new 4GB, RAID 5 logical drive composed of three physical drives. The 4GB increased capacity (2G from each new member; parity drive's capacity is discounted) appears as a new partition.

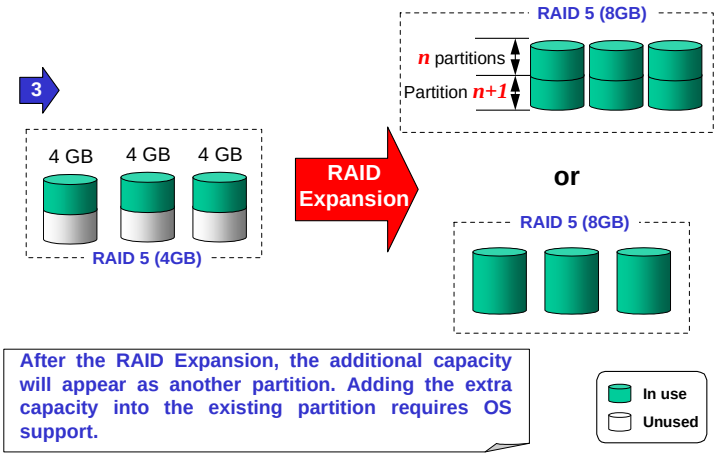


Figure 9-6: RAID Expansion Mode 2 (3/3)

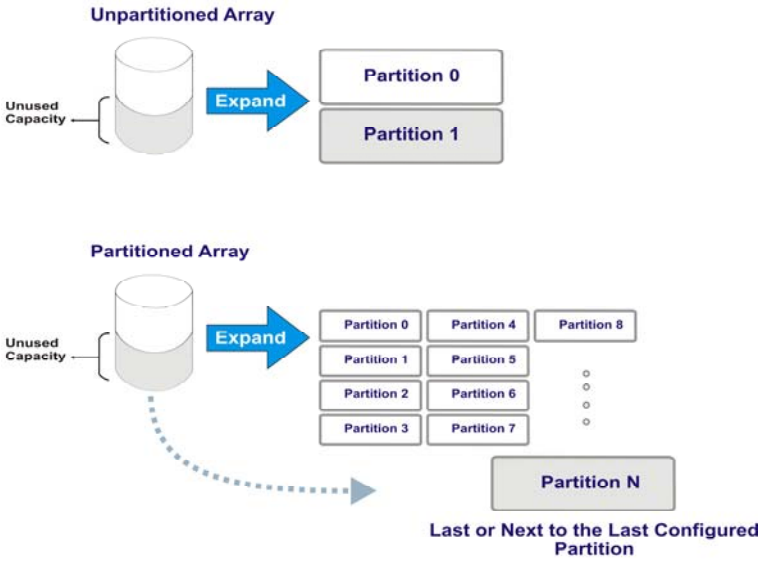
IMPORTANT!

The increased capacity from either expansion type will be listed as a new partition.

CAUTION!

1. If an array has not been partitioned, the expansion capacity will appear as an added partition, e.g., partition 1 next to the original partition 0.

2. If an array has been partitioned, the expansion capacity will be added behind the last configured partition, e.g., partition16 next to the previously-configured 15 partitions.
3. If an array has been partitioned by the maximum number of partitions allow, the expansion capacity will be added to the last partition, e.g., partition 63. Partition change **WILL INVALIDATE** data previously stored in the array.
4. See the diagram below for the conditions that might occur during array expansion.



The new partition must be mapped to a host ID/LUN in order for the HBA (host-bus adapter) to see it.

9.2.5 Adding Spare Drives

You can assign spare drives to a logical drive to serve as backups for failed drives. In the event of a drive failure, the spare drive will be automatically configured into the array and reconstruction (or rebuilding) will immediately commence.

Multiple spare drives can co-exist in an enclosure; however, this configuration is rarely used due to its high cost and the uncommon occurrences of drive failures. A practical configuration calls for one spare drive per logical drive. After a failed drive is rebuilt, replace the failed drive and then configure the replacement as the new spare drive.

NOTE:

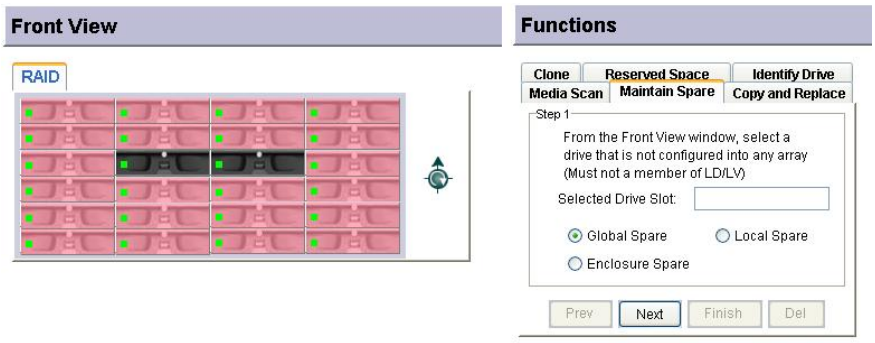
Adding a spare drive can be done automatically by selecting the RAID 1+Spare, RAID 3+Spare, RAID 5+Spare or RAID 6+Spare option from

the logical drive RAID Level selection dialog box during the initial configuration process. These options apply to RAID 1, RAID 3, RAID 5 and RAID 6 levels respectively.

9.2.5.1. Accessing the Spare Drive Management Screen

To open the **Spare Drive Management** screen, please follow these steps:

Step 1. Select the logical drive to which you wish to add a dedicated spare from the list of the logical drives above. In the Functions window, click the **Maintain Spare** tab. The functional window is accessed from the Physical Drives window as shown in *Error! Reference source not found.*, the **Maintain Spare** button appears.



Step 2. From the **Front View** window, select the disk drive you want to use as a dedicated spare, Global, or Enclosure spare with a single mouse-click.

Step 3. After selecting the drive that will be used as a spare, the selected drive's slot number will be displayed and you may click the **Next** button to complete the process.

Step 4. If you prefer to create a dedicated spare, you will need to specify a logical drive to which the dedicated spare belongs.

NOTE:

An Enclosure Spare is one that is used to rebuild all logical drives within the same enclosure. In configurations that span across multiple enclosures, a Global spare may participate in the rebuild of a failed drive that resides in a different enclosure. Using Enclosure Spare can avoid disorderly locations of member drives if members reside in different enclosures.

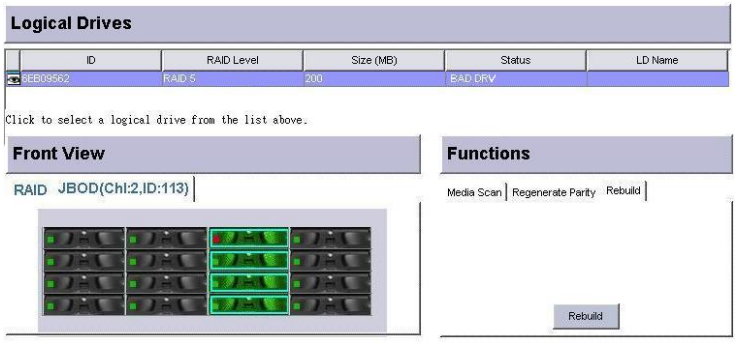
9.2.6 Rebuilding Logical Drives

Depending on the presence of a spare drive, rebuild is initiated automatically or must be started manually. In the presence of a spare drive, the system automatically commences a rebuild using the spare drive. This process is done in the background, and thus transparent to the users. However, in either case you should replace the failed drive as soon as possible and insert a new drive and configure it as a spare just in case another drive may fail and you will need a spare drive.

In the absence of a spare drive, rebuild is manually started. Before initiating a manual rebuild, you must first replace the failed drive. If you install the replacement drive in the same drive slot (that is, the same channel and ID), then you can proceed with the rebuilding process by clicking on the **Rebuild** button; otherwise, you may need to scan in the drive first.

A failed drive should be replaced as soon as possible. For a RAID 3 or RAID 5 array, two failed members will cause an irrecoverable loss of data.

The controller/subsystem can be set to rescan the drive bus for a replacement drive at preset intervals. The related setting can be found in **Configuration Parameters** -> **Other** -> **Drive Side Parameters** -> **Drive Fail Swap Check Period** in second.



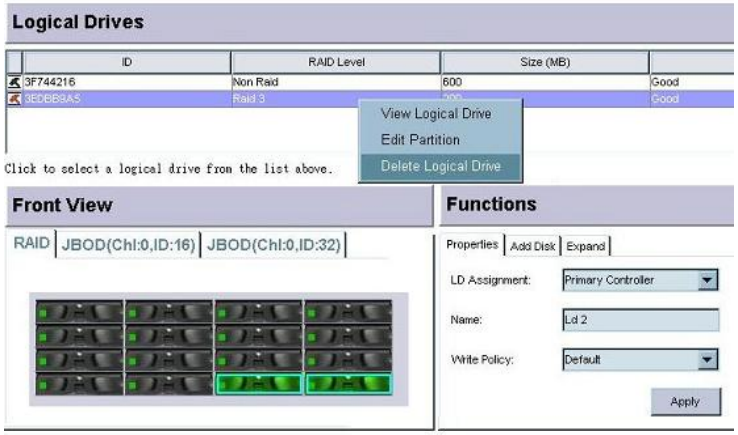
9.2.7 Deleting an LD

If you want to delete an LD from your RAID subsystem, follow the steps outlined below. Remember that deleting an LD results in destroying all data on the LD.

IMPORTANT!

Deleting a logical drive irretrievably wipes all data currently stored on the logical drive.

Step 1. Select the logical drive you wish to remove with a single mouse-click. **Right-click** on the adjacent screen area. A command menu will prompt as shown below**.**



Step 2. Select the **Delete Logical Drive** command. The delete process is completed almost immediately.

Step 3. Once the **Delete** command has been selected, a confirm box will prompt asking you whether to proceed or not.

Step 4. If you are certain that you wish to delete the LD, press the **OK** button. If you are not sure, click the **Cancel** button.

9.3. Logical Volume Management

Combining logical drives together creates logical volumes. You can combine logical drives with different capacities and RAID levels into a single logical volume.

NOTE:

When you delete a logical volume, all logical drives assigned to it will be released, making them available for new logical volume creation.

9.3.1 Accessing the Create Logical Volume Window

Logical Volumes are created in the **Create Logical View** window, which can be accessed either from the navigation panel icon or the command menu on the software menu bar.

Step 1. To create Logical Volumes; display the **Create Logical Volume** window by clicking on the associated icon in the GUI's navigation panel or the command in the **Action** menu bar.

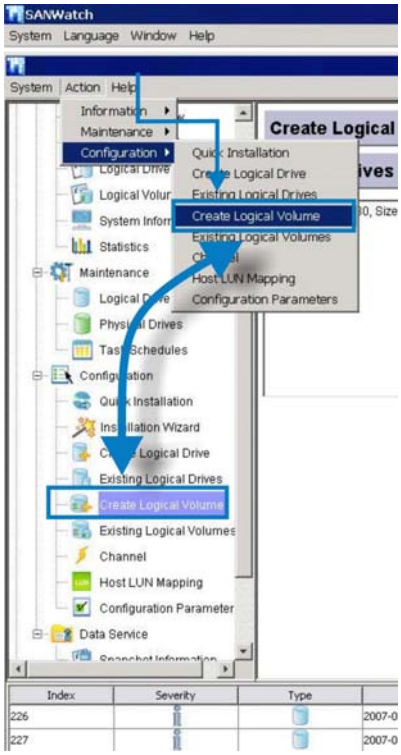
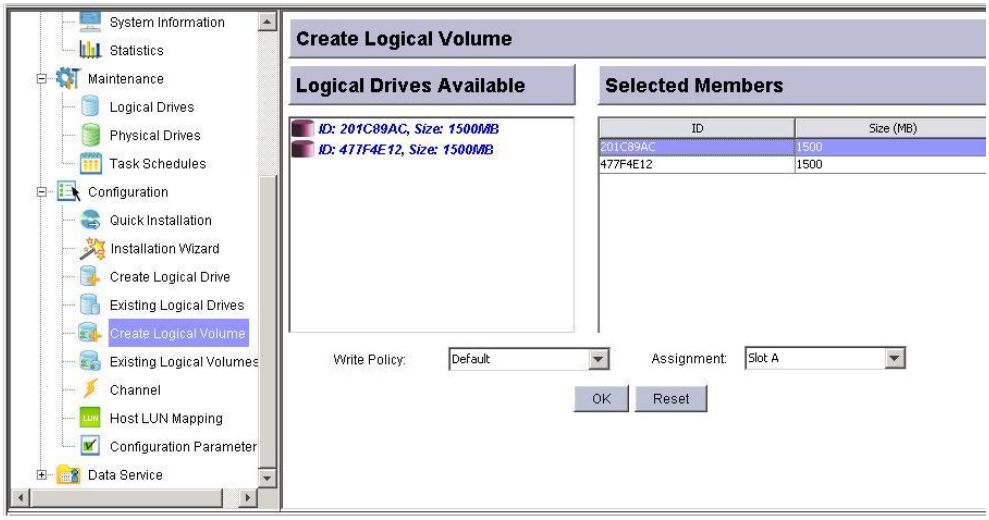


Figure 9-7: Accessing the Create Logical Volume Window

Step 2. The **Create Logical Volume** window will appear.



9.3.2 Creating Logical Volumes

9.3.2.1. LV Creation

Step 1. Select the LDs that will be used in the LV from the **Logical Drives Available** panel.

Step 2. Select the following RAID parameters:

- Write Policy
- Assignment

Step 3. Information about the selected LDs will appear on the **Selected Members** panel. Click the **OK** button.

9.3.2.2. Selecting LDs

Step 1 Select each logical drive you wish to include in the new logical volume with a single mouse-click. Select the Logical Drives you wish to incorporate into a Logical Volume and click the **Add** button beneath the **Available** menu.

Step 2. All available logical drives are listed on the left. Double-check to ensure that you have selected the appropriate members.

9.3.2.3. Setting Logical Volume Parameters

Logical Volume parameter options can be accessed at the lower half of the **Create Logical Volume** window.

Logical Volume Assignment

Select Slot A controller or Slot B controller from the Logical Volume Assignment menu.

NOTE:

In a single-controller configuration or the BIDs (Slot B controller IDs) are not assigned on host channels, the LD Assignment menu will not be available.

Select Write Policy

Use the **Write Policy** menu to select Default (Global Setting), Write Through, or Write Back. The same policy will automatically apply to all logical drives (members) included in the logical volume.

NOTE:

The **Default** option should be considered as "**Not-Specified**." If set to Default, the logical drive's caching behavior will be automatically controlled by firmware. In the event of component failure or violated temperature threshold, the Write-back caching will be disabled and changed to a more conservative "Write-through" mode.

9.3.2.4. Click OK to Create a Logical Volume

Once the logical drives that will be used in the Logical Volume have been selected and all the desired Logical Volume parameters have been selected:

Step 1. Click the **OK** button at the bottom of the **Create Logical Volume** window.

Step 2. The creation is completed almost immediately.

9.3.3 Accessing the Existing Logical Volumes Window

The **Existing Logical Volumes** window allows you to perform Logical Volume expansion and change related configuration options. As shown below, the configuration window can be accessed either from the functional navigation panel or the command menu on the top of the GUI screen.

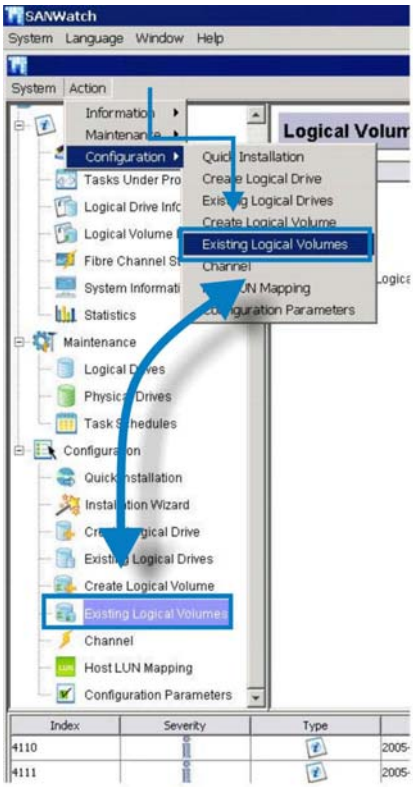
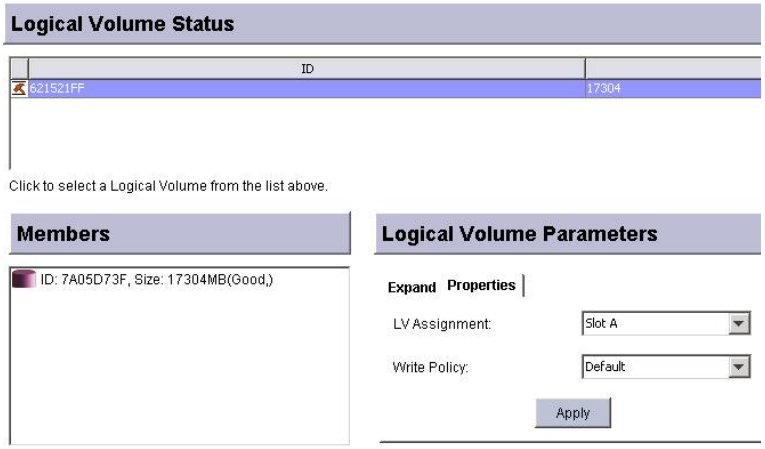


Figure 9-8: Accessing Existing Logical Volume Window

9.3.3.1. Modifying Logical Volume Configurations

Some configurations can be modified in the **Properties** command page. To access the page, select a Logical Volume and click on the **Properties** tab under the **Functions** window.



Each option is executed by a two-step procedure. Click to select a desired value from the pull-down menu, and then click **Apply** for the configuration to take effect.

LV Assignment: both controllers can access a logical volume. In traditional LV management, one LV can only be accessed by primary or secondary controller. For systems running later firmware releases, assignment is made by the locations of RAID controllers, i.e., Slot A or Slot B controller.

Write Policy: Write policy can be adjusted on a per logical volume basis. This option allows you to set a write policy for the specific logical volume. "Default" is a neutral value that is coordinated with the controller's general caching mode setting. Other choices are "Write-back" and "Write-through."

9.3.3.2. Expanding a Logical Volume

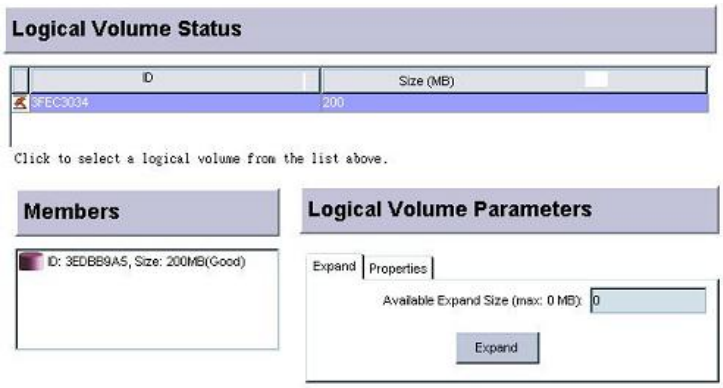
When members of a logical volume have free and unused capacity, the additional capacity can be added to existing logical volumes. The unused capacity can come from the following configuration:

- Certain amount of capacity was intentionally left unused when the logical drives were created (configurable with maximum array capacity).

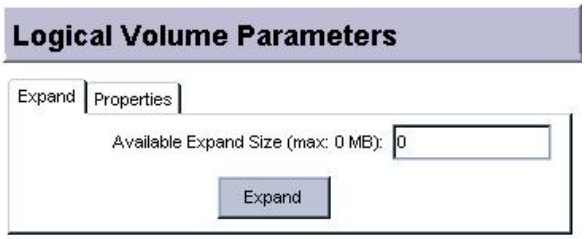
- Some or all of the members of a logical volume have been expanded, either by adding new drives or copying and replacing original drives with drives of larger capacity.

9.3.3.3. Accessing the Expand Logical Volume Page

Step 1. Select a configured Logical Volume from the **Existing Logical Volumes** window shown below. All existing Logical Volumes will appear on the **Logical Volume Status** panel.



Step 2. The expand command can be found by clicking the **Expand** tab under the **Logical Volume Parameters** panel.



Step 3. Available expansion size displays in a text box if there is any amount of unused capacity.

Step 4. Click the **Expand** button at the bottom of the configuration panel. The expand process should be completed in a short while because all unused capacity in the members of a logical volume must have been made useful through the similar expansion process. The expansion process on a logical volume simply lets subsystem firmware recognize the change in the arrangement of free capacity.

NOTE:

You may combine partitions under **View and Edit Logical Volume Partition Table** by expanding the size of earlier partitions (such as increasing the size of partition 0 so that it is as large as all partitions combined to make one partition).

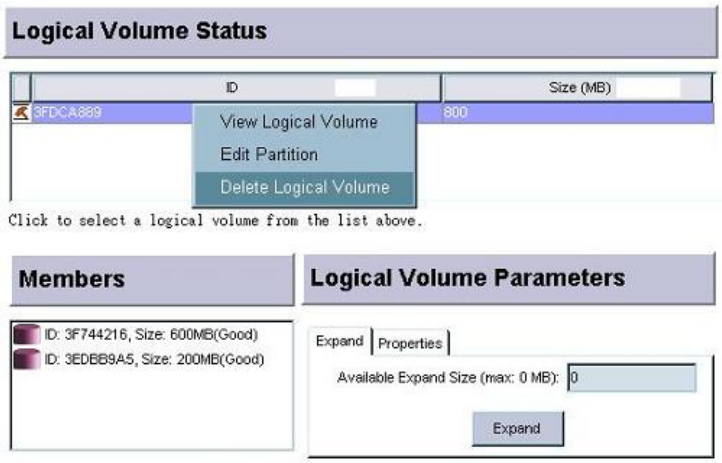
WARNING!

Combining partitions destroys existing data on all drive partitions.

Step 5. The logical volume will now have a new partition the same size as the expansion. **Right-click** the expanded volume and select the **Edit Partition** command to check the result of the expansion.

9.3.4 Deleting a Logical Volume

Step 1. Select the configured volume you wish to remove with a single mouse-click. **Right-click** the adjacent area to display a command menu. All Logical Volumes will appear below the **Logical Volume Status** panel.



Step 2. You will be asked to confirm that you wish to delete the selected Logical Volume. If you are certain that you want to delete the Logical Volume then select **OK**. The logical volume will be deleted and removed from the logical volumes list.

9.4. Partitioning a Logical Configuration

9.4.1 Overview

Partitions can be created in both logical drives and logical volumes. Depending on your specific needs, you can partition a logical drive or logical volume into two or more smaller-size partitions or just leave it at its default size (that is, one large partition covering the entire logical drive or logical volume).

If you intend to map an entire logical drive or logical volume to a single host LUN, then partitioning becomes irrelevant. Partitioning can be helpful when dealing with arrays of massive capacities and when rearranging capacities for applications that need to be accessed by many application servers running heterogeneous OSes.

NOTE:

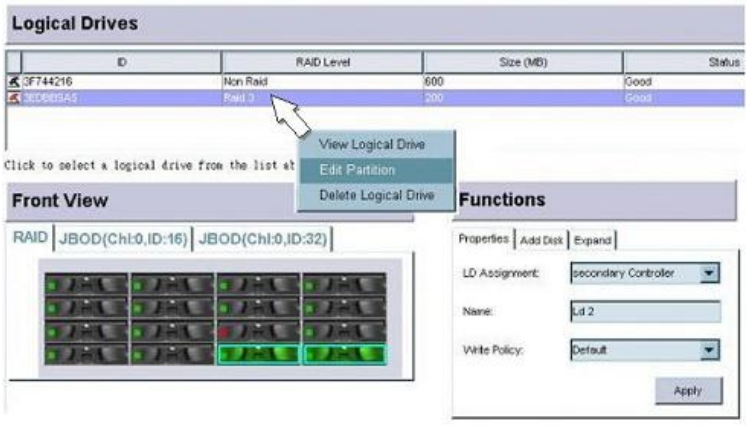
You can create a maximum of eight partitions per logical drive or logical volume. Also, partitioned logical drives cannot be included in a logical volume.

9.4.2 Partitioning a Logical Drive

WARNING!

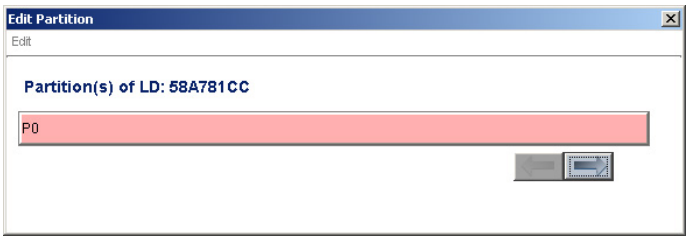
Partitioning a configured array destroys the data already stored on it. Partitioning is recommended during the initial setup of your subsystem. You have to move your data elsewhere if you want to partition an array in use.

Step 1. Select the logical drive you want to partition. Move your cursor to the **Logical Drives** window. **Right-click** to display the Edit Partition command menu.



Step 2. Select **Edit Partition** from the menu.

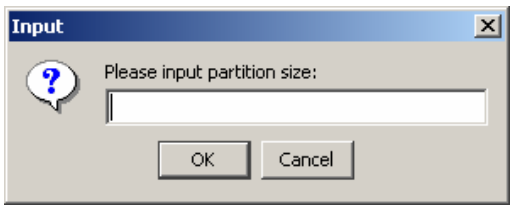
Step 3. The **Edit Partition** window displays. Use the arrow keys on the button on the lower right to switch between partitions.



Step 4. If the array has not been partitioned, all of its capacity appears as one single partition. Single-click to select the partition (the color bar).

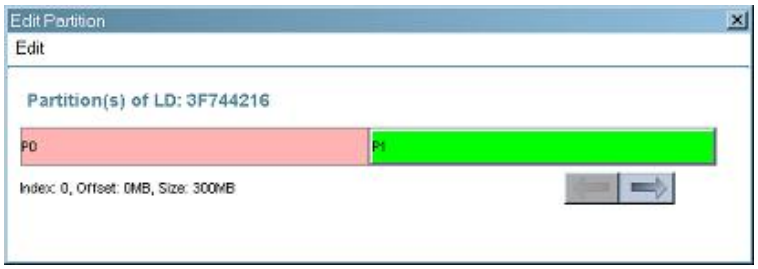
Step 5. **Right-click** or select the **Edit** command to display the **Add Partition** command. Click to proceed.

Step 6. The **Partition Size** window displays. Enter the desired capacity and press OK to proceed.



Step 7. Shown below is a capacity partitioned into two. Each partition is displayed in a different color. Repeat the above process to create more partitions or click to view its

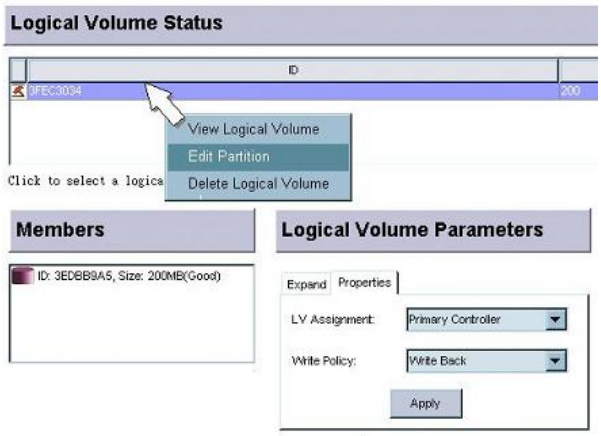
information. A new partition is created from the existing partition.



The **arrow** buttons help you travel from one partition to another.

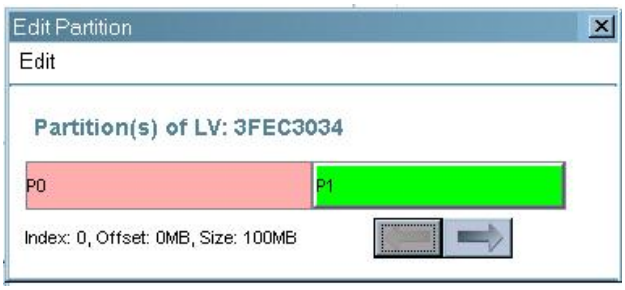
9.4.3 Partitioning a Logical Volume

Step 1. Select the logical volume you wish to partition. Move your cursor onto the **Logical Volume Status** window. **Right-click** to display the Edit Partition command menu.



Step 2. Select **Edit Partition** from the menu.

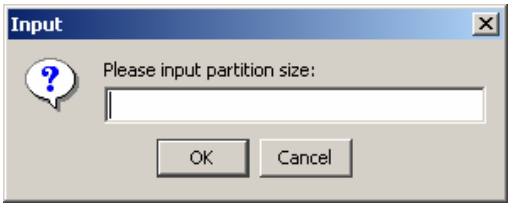
Step 3. The **Edit Partition** mode window displays as shown below.



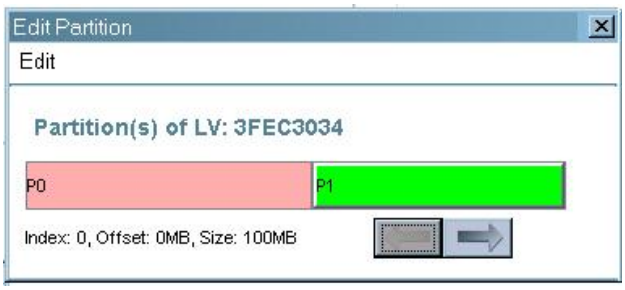
Step 4. If the volume has not been partitioned, all of the array capacity appears as one single partition. Single-click to select a partition from the color bar.

Step 5. **Right-click** or select the **Edit** command to display the **Add Partition** command. Click to proceed.

Step 6. The **Partition Size** window displays. Enter the desired capacity (1/2 or 1/3 of the original volume capacity, for example) and press **OK** to proceed.



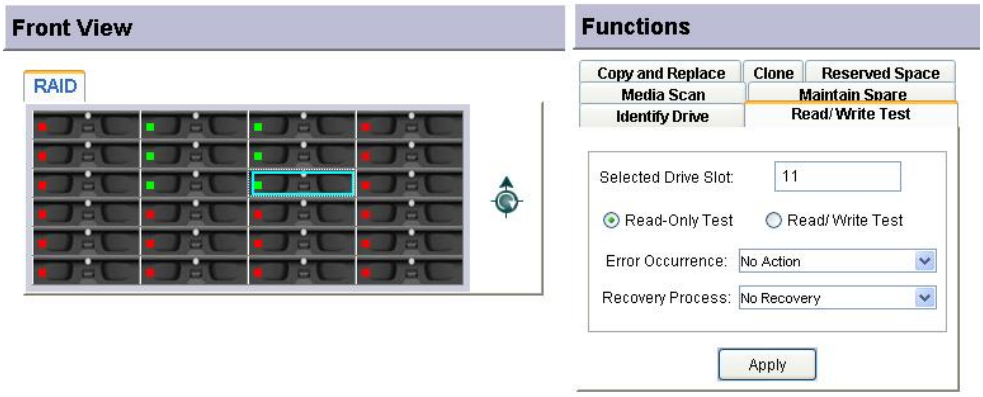
Step 7. Shown below is a capacity partitioned into two. Each partition is displayed in a different color. Repeat the above process to create more partitions or click to view its information.



The **arrow** buttons help you travel from one partition to another.

9.5. Physical Drive Maintenance

9.5.1 Read/Write Test



Step 1. To access the **Read/Write Test** maintenance option, select the **Physical Drives** icon from the functional navigation panel on the left of the SANWatch screen.

Step 2. Select a new drive from the **Front View** window. A used drive (one that previously included in a logical configuration) can also be tested with the precondition that its reserved space needs to be manually removed.

Step 3. Select **Read/Write Test** from the tabbed menus in the **Functions** window.

Step 4. Verify the listed drive slot number. Select the Test type as either **Read-only** or **Read/Write** test.

Step 5. There are two configurable parameters related to the Read/Write test: **Error Occurrence** and **Recovery Process.**

Use the pull-down menu to configure a preferable test condition. The configurable options are listed below:

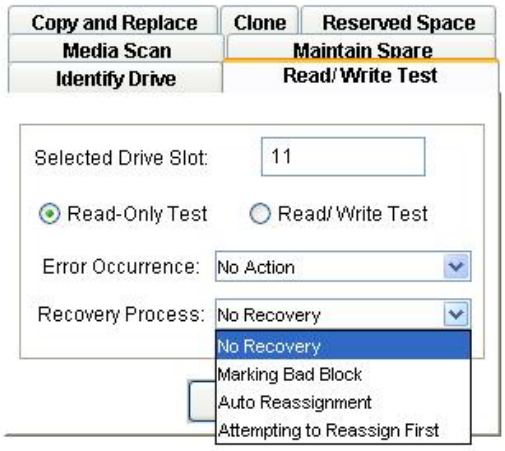
Error Occurrence: This item specifies firmware's reactions if any errors should be found during the Read/Write test. Options are: **No Action**, **Abort on Any Error**, **Abort on Hardware Errors**.

Note that the definitions of drive errors are determined by the interface type. For SATA disk drives, errors are interpreted according to SATA 8-bit error encoding.

Recovery Process: Firmware might attempt to correct some of the errors discovered on drives. The configurable options are:

No Recovery, **Marking Bad Block**, **Auto Reassignment**, and **Attempting Reassign First**.

If selected, the last option will attempt to reassign bad blocks, and if the reassignment fails, mark those drive sectors as **BAD**.



Chapter 10
LUN Mapping

After creating a logical drive (LD) or logical volume (LV), you can map it as is to a host LUN; or, if the array is divided into smaller partitions, you can map each partition to a specific host LUN. SANWatch supports many LUNs per host channel, each of which appears as a single drive letter to the host if mapped to an LD, LV, or a partition of either. In cases where certain mappings are found to be useless, or the disk array needs to be reconfigured, you can delete unwanted mappings in your system.

This chapter explains the following LUN mapping features:

- **Accessing the LUN Map Table – Section 10.1**
- **LUN Mapping – Section 10.2**

  10.2.1 Mapping a Complete Logical Drive or Logical V

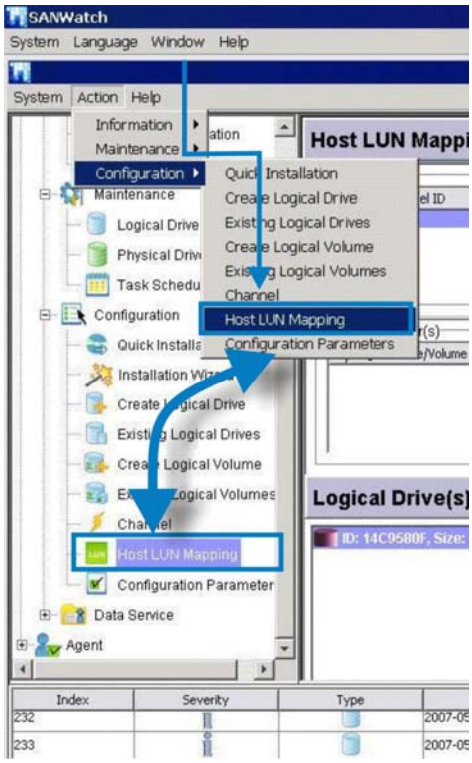
  10.2.2 Map a Logical Drive or Volume Partition to a Host LUN

  10.2.3 Deleting a Host LUN Mapping

10.1. Accessing the LUN Map Table

The LUN Map Table lists the logical drives, logical volumes and array partitions that have previously been mapped. To access the LUN Map Table, please follow these steps:

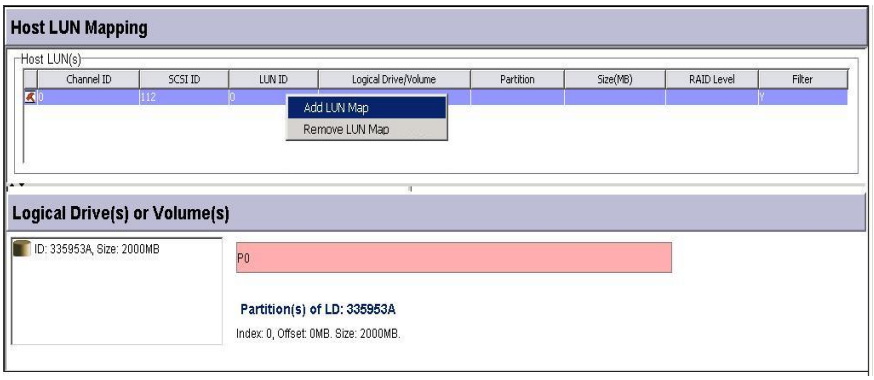
Step 1. In the navigation panel under the **Configuration** category, click on the **Host LUN Mapping** where you can find the configuration options with the mapping operation.



Step 2. The Host LUN Mapping window will appear on the right. Right-click on the Host LUN(s) sub-window to display the command menu. Select either a Slot A ID or a Slot B ID. Infortrend's controllers or subsystems always come with pre-configured IDs.

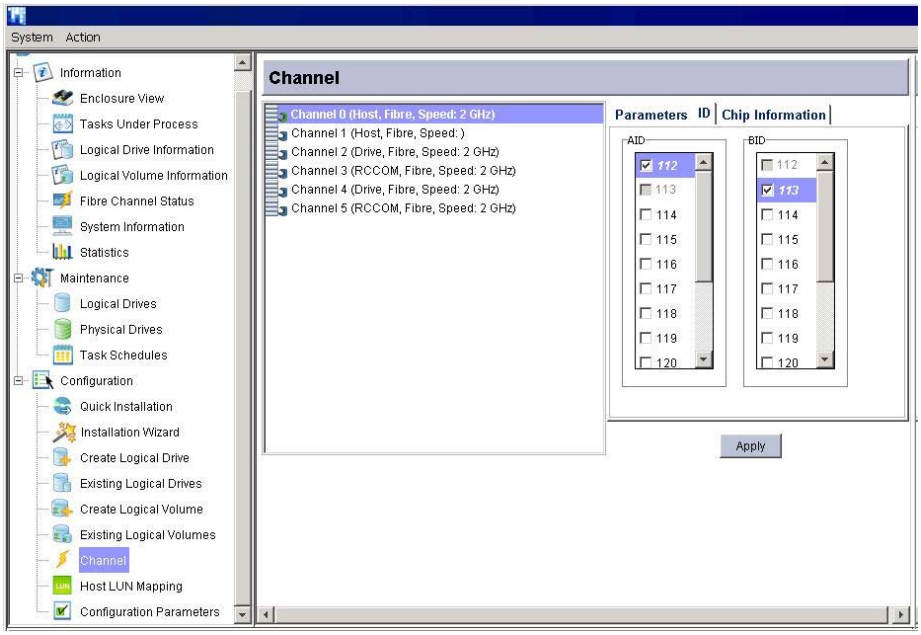
If it is necessary to create alternative IDs, please select the **Channel** icon from the navigation panel to enter the Channel configuration menu.

Step 3. Right-click to display and execute the **Add LUN Map** command.



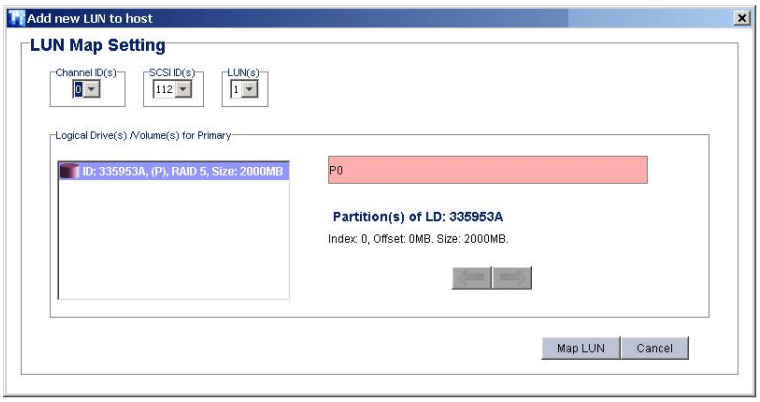
In a redundant-controller configuration, you will be prompted to select either a **Slot A** controller or a **Slot B** controller. When RAID arrays are equally assigned to the partner controllers, workload can be shared between the RAID controllers.

Options with Controller A or Controller B ID



The Channel Window: where you manually add or remove a channel ID.

Step 4. After selecting a RAID controller whose host ID will be used in the following process, the **LUN Map Setting** window appears as shown below.



10.2. LUN Mapping

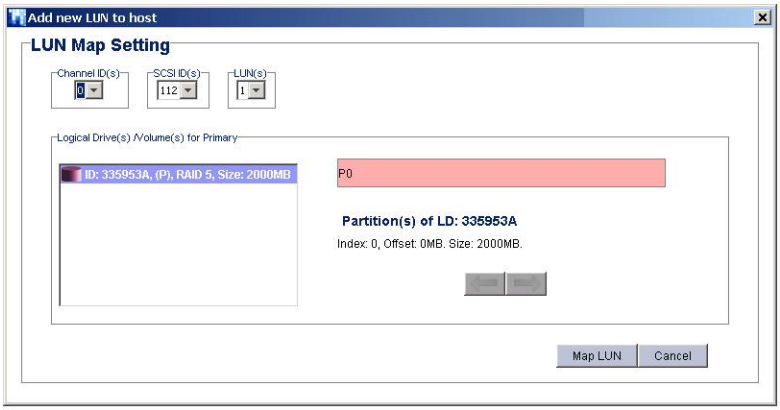
10.2.1. Mapping a Complete Logical Drive or Logical Volume

Step 1. Follow the steps listed in ***Section 10.1*** above to access the **Host LUN Mapping** window..

Step 2. Select the appropriate **Channel**, **Host ID**, and **LUN** numbers from the separate pull-down lists.

Step 3. Select a Logical Drive or Logical Volume and then select a partition from the Partition color bar by a single mouse-click. The partition bar appears on the right-hand side of the screen. Carefully check the partition's index number before making the host LUN mapping.

Step 4. Click on the **Map LUN** button to complete the process.



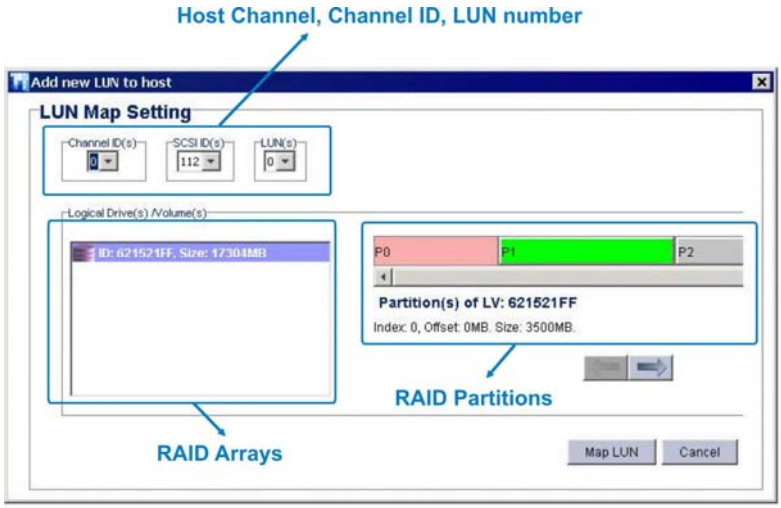
10.2.2. Map a Logical Drive or Volume Partition to a Host LUN

Step 1. First, make sure your logical drives or logical volumes have been appropriately partitioned.

Step 2. Follow the steps listed in ***Section 10.1*** above to access the **LUN Map Setting** window.

Step 3. When the LUN Map window appears, select the appropriate **Channel** number, channel **ID**, and **LUN** numbers from the separate pull-down lists above.

Step 4. Select a Logical Drive or Logical Volume with a single mouse-click. With a single mouse-click on the Partition color bar, select one of the partitions that you wish to associate with the selected channel ID/LUN number.

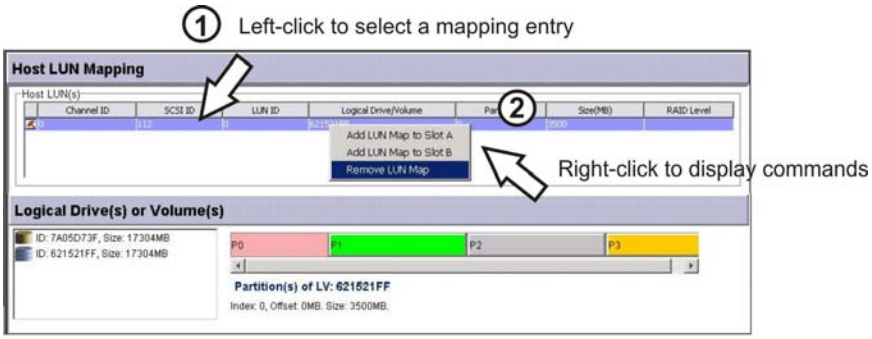


Step 5. Click on the **Map LUN** button to complete the process.

10.2.3. Deleting a Host LUN Mapping

Step 1. Follow the steps listed in ***Section 10.1*** above to access the **LUN Map Setting** window.

Step 2. **Left-click** on a configured LUN and then **right-click** on the high-lighted area. A command menu displays. Select **Remove LUN Map** to complete the process.



Step 3. When prompted for a password or an answer, enter it and click **OK**. The LUN mapping should no longer be listed in the **LUN Map** table. After deleting the LUN mapping it no longer appears in the host LUN(s).

Step 4. To remove additional LUN mappings, repeat the above procedure.

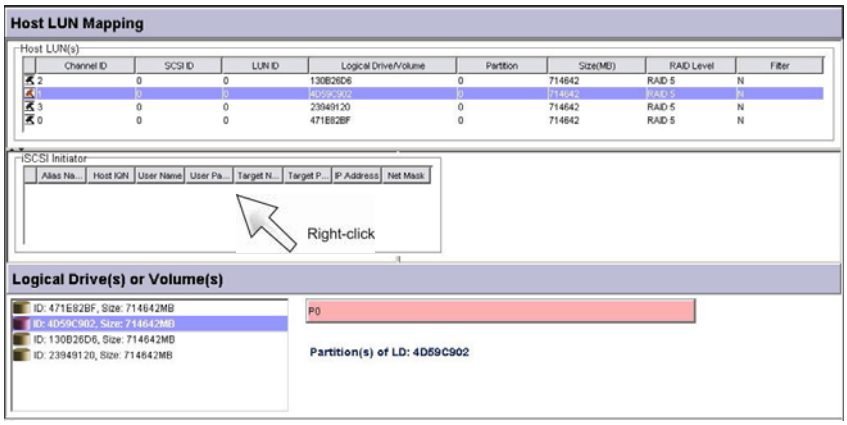
10.2.4. LUN Mapping Access Control over iSCSI Initiator Settings

For subsystems featuring iSCSI host interfaces, an access control list will be available with the host LUN mapping screen.

The iSCSI Initiator settings allow you to associate or disassociate a specific initiator with specific RAID volumes. Two-way (Mutual) CHAP can also be implemented here. With the associated settings, you can apply access control over iSCSI network for ensuring data security.

NOTE:

Before configuring One-way and Two-way CHAP, you need to enable the CHAP option in the "Configuration Parameters"→ "Host-side" Parameters window.



Step 1. To access the iSCSI initiator settings menu, **right-click** on the iSCSI Initiator column to bring out the configuration menu (shown above and below).

Step 2. Follow the details in the table below and enter appropriate information and values to establish access control.

Table 10-1 iSCSI Initiator CHAP Configuration Entries

Host Alias Name	Enter a host alias name to specify a CHAP association with a specific software/hardware initiator. This Alias name facilitates ease of recognition because iSCSI initiator IQN consists of many characters and is often too long to remember.
Host IQN	In here you can manually enter an initiator's IQN (iSCSI Qualified Name); *- or –* Select from the list of connected initiators by clicking on the pull-down button to display the currently connected initiators.
User Name	The user name here applies to a one-way CHAP configuration. Identical name and password must be configured on the initiator software or HBA configuration utility. User/target name and password are used for the inbound authentication processes between the called and calling parties. Names and passwords are identical here and at the initiator side.
User Password	The user password here applies to a one-way CHAP configuration for inbound authentication. Note that some CHAP configuration utilities may use "secret" instead of "password."
Target Name	The target name here applies to a two-way (mutual) CHAP configuration. Identical target name and password must be configured on the initiator software or HBA configuration utility.
Target Password	The target password here applies to a two-way CHAP configuration for outbound authentication.
IP Address	Enter the IP address of an iSCSI initiator.
NetMask	Enter an appropriate NetMask value here.

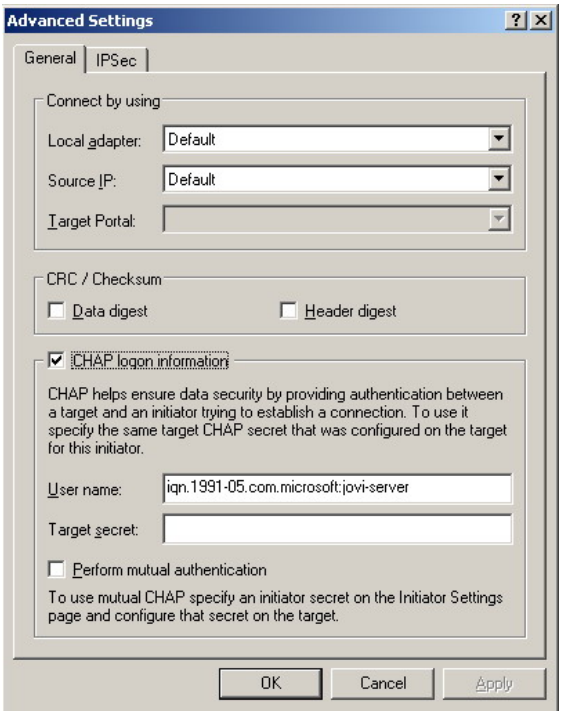
NOTE:

Some login authentication utilities provided with iSCSI HBAs on Windows operating systems require a CHAP password of the length of at least 12 characters.

NOTE:

1. Infortrend supports one-way or two-way (mutual) CHAP authentication. With two-way CHAP, a separate three-way handshake is initiated between an iSCSI initiator and storage host port.

   On the initiator side (for example, Microsoft initiator software), CHAP logon is designated as an option with selectable initiator IQN name and that of the target secret (to which the CHAP authentication call will be issued; namely, the host port on your subsystem).


Advanced Settings
General
IPSec
Connect by using
Local adapter:
Default
Source IP:
Default
Target Portal:
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator trying to establish a connection. To use it specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:jovi-server
Target secret:
Perform mutual authentication
To use mutual CHAP specify an initiator secret on the Initiator Settings page and configure that secret on the target.
OK
Cancel
Apply

2. Microsoft iSCSI initiator uses IQN as the default User name for CHAP setting. A different User name can be specified here instead of the default.

3. For more information on CHAP-related settings, please refer to the documentation that came with your initiator hardware or software drivers.

This page is intentionally left blank.

Chapter 11

System Monitoring and Management

- **RAID Information – Section 11.1**
  - **The Information Category**
  - **Date and Time**
- **Enclosure View – Section 11.2**
  - **Task Under Process**
  - **Event Log List/Configuration List Window**
- **Logical Drive Information – Section 11.3**
  - **Accessing Logical Drive Information**
- **Logical Volume Information – Section 11.4**
  - **Accessing Logical Volume Information**
- **Fibre Channel Status – Section 11.5**
- **System Information – Section 11.6**
- **Statistics – Section 11.7**

11.1 RAID Information

Unlike its predecessor, SANWatch presents access to all information services under one Array Status category. Users logged in using the Information authorization will be allowed to access the information windows while being excluded from other configuration options.

Support for device monitoring via SAF-TE, SES, and I^2C data buses is the same. However, SANWatch now uses a more object-oriented approach by showing the enclosure graphics, which are identical to your EonRAID or EonStor enclosures. SANWatch reads identification data from connected arrays and presents a correct display as an enclosure graphic. This process is automatically completed without user's setup.

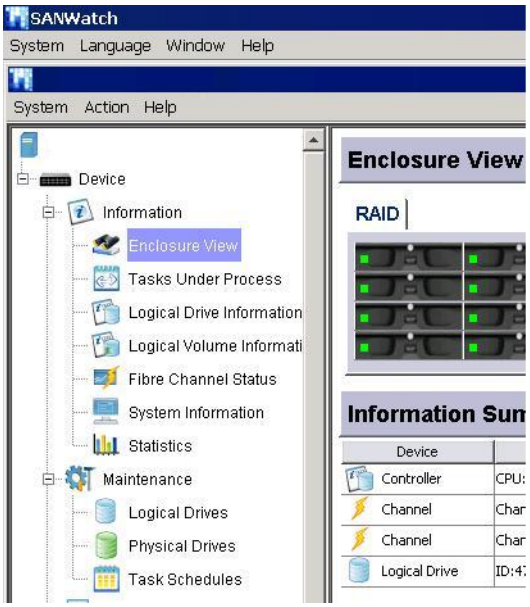
NOTE:

SANWatch does not support the display of drive enclosures provided by other vendors.

The Information Category

Once properly set up and connected with a RAID array, a navigation panel displays on the upper left of the screen. SANWatch defaults to the Enclosure View window at startup.

To access each informational window, single-click a display icon on the navigation panel. You may also access each window by selecting from the **Action** menu on the menu bar at the top of the screen. See below for access routes.



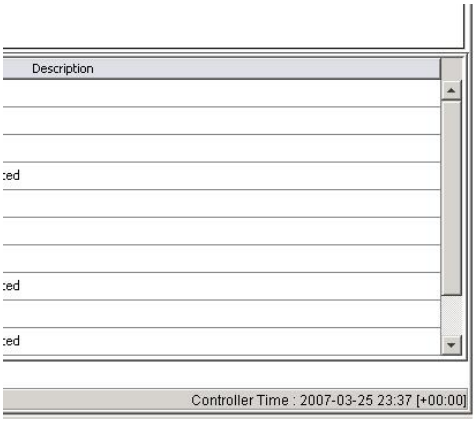
The Array Information category provides access to seven display windows as listed below:

Icon	Description
	Icon for the Array Information category
	Opens the **Enclosure View** window
	Displays the **Configuration Tasks** currently being processed by the subsystem
	Opens the **Logical Drive** information window
	Opens the **Logical Volume** information window
	Opens the **Fibre Channel Status** window
	Opens the **System View** window
	Opens the **Statistics** window

Table 11-1: Array Information Icons

Date and Time

Once date and time has been configured on your subsystem, they are displayed on the bottom right corner of the manager's screen.



Maintaining the system date and time is important, because it is used for tracking a pending task, past events, configuring a maintenance task schedule, etc. Date and time are generated by the real-time clock on the RAID controller/subsystems.

11.2 Enclosure View

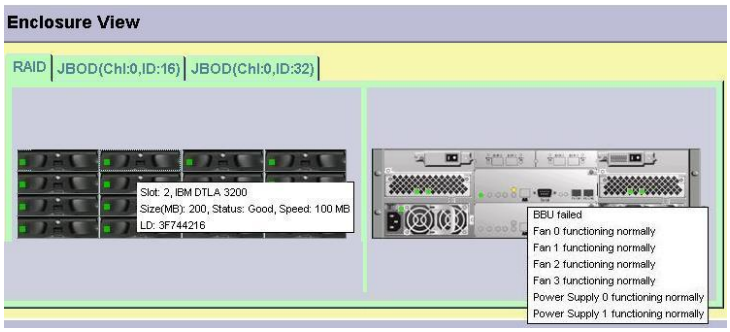
The Enclosure View window displays both the front and the rear views of connected enclosures. For the EonStor subsystems, SANWatch displays drive trays in the front view, and system modules (power supplies, cooling modules, etc.) in the rear view. For the EonRAID controllers, SANWatch displays FC port modules and LEDs in the front view; powers supplies, cooling modules, and controller modules display in the rear view.

If multiple enclosures are cascaded and managed by a RAID subsystem, SANWatch defaults to the display of RAID enclosures and the graphics of the cascaded JBODs, which can be accessed by clicking the tab buttons.

SANWatch is capable of displaying any information provided by an SES, SAF-TE or I^2C data bus. Various kinds of information is typically provided including the status of:

- Power supplies
- Fans
- Ambient temperature
- Voltage
- UPS
- Disk drives
- System module LEDs

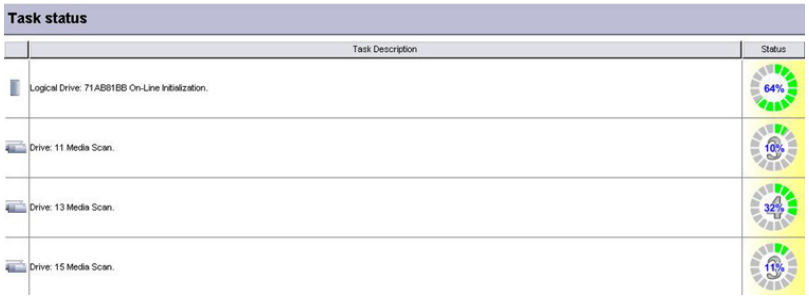
To read more information about enclosure devices, place your cursor either over the front view or rear view graphic. An information text field displays as shown below.



More information about each enclosure device can also be found in the System Information window.

Task Under Process

Access the Task Under Process window by clicking on the display icon in the SANWatch navigation panel.



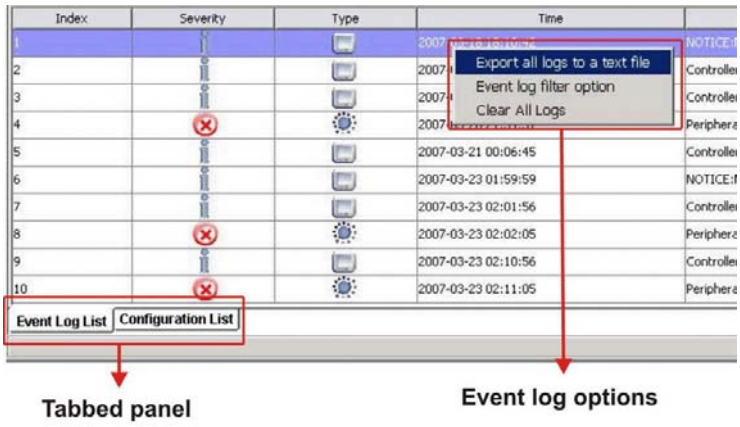
- This window shows the unfinished tasks currently being processed by the subsystem. The Task Status display includes disk drive maintenance tasks such as Media Scan or Regenerate Parity, and array configuration processes such as logical drive initialization and capacity expansion.

- If you find that you have made the wrong configuration choice, you may also left-click and then right-click on the task information to display the **Abort** command.

- A brief task description, start time, and a percentage indicator are available with each processing task.

Event Log List/Configuration List Window

In the bottom of SANWatch program shows **Event Log List** and **Configuration List** windows. You can switch between the two windows by clicking on the tabbed panel on the bottom left of SANWatch screen.



Event Log List Window

The **Event Log List** window generates the system's event log list at the bottom of the SANWatch screen. The Event Log window gives users the real-time monitoring, alerting as well as status reporting of the RAID systems.

When a new event is generated, the icon under **Severity** column will flash to draw user's attention. The severity icons also indicate the severity level of an event. (See ***Table 11-2***) You can easily read the time of an event occurred by viewing the **Time** column.

Icon	Definition	Explanation
	Information	A notice of an action begin/complete or status change of the RAID system.
	Warning	This is a warning message that an event happened that may cause damage to the system.
	Critical	A critical condition happened. SANWatch program strongly suggest you to check your system immediately.

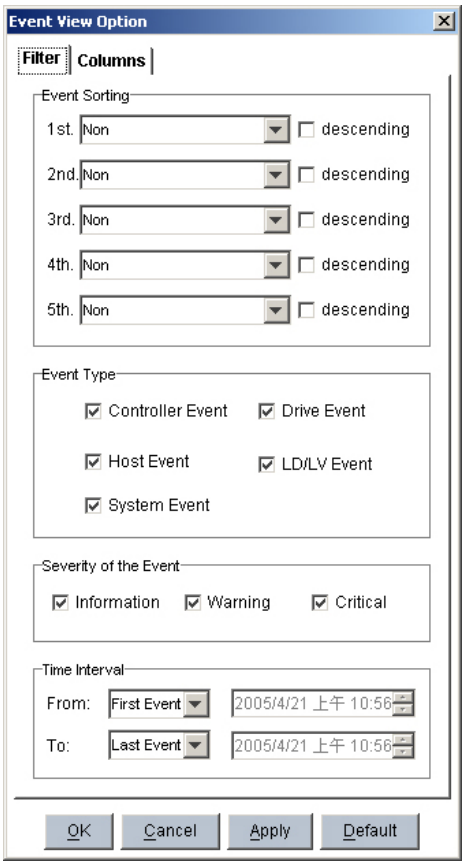
Table 11-2: Severity Level Icons

The Event log list function allows you to export the logs to a text file, and the event log filter option enable users to easily filter stores of log files for specific event logs and then view, filter, export, and report on the events of interest.

To export or filter the event logs, right-click on the event log list window. Three selections will appear on the screen. You may select **Export all logs to a text file**, **Event log filter option** or **Event log clear option**.

- **Export All Logs to a Text File**: This option will export all logs start from the time you accessed the RAID system to a text file. You may select a location where you like to save the file in a **Save** window. If you like to export any specific events, set the **Event log Filter** option before export the logs to a text file.

- **Event Log Filter Option**: When you click this option, an Event View Option window will prompt up.



In the **Event View Option** window, the tabbed panel on the top of the window allow you to switch between the **Filter** and **Column** pages.

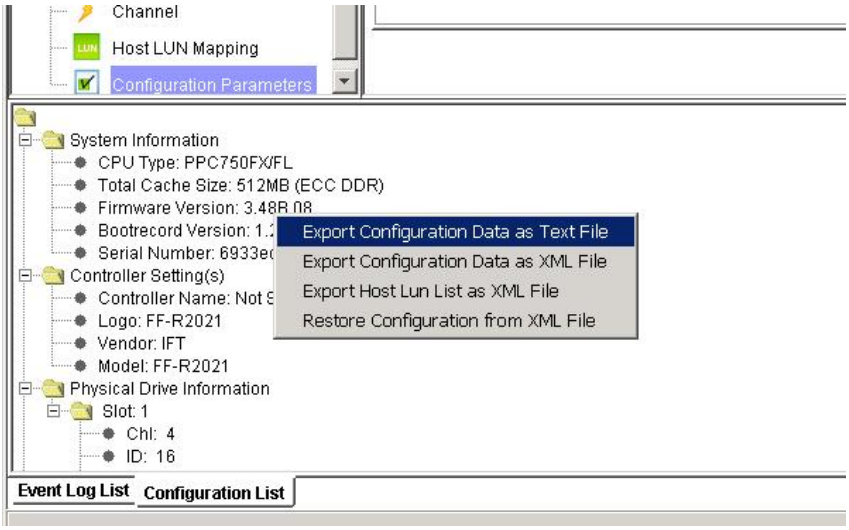
You may set the event sorting criteria, the type of events you like to export, the severity of the event and the time occurrence range in the **Filter** page of the **Event View Option** window. The **Column** page allows you to select the related display items when showing the events. Click **Apply** for the changes to take effect. The **Event Log List** window will immediately display the event list following the new criteria. Click **OK** to exit the window, or click **Default** to return to the system default settings.

- **Event Log Clear Option**: This option allows you to clear the event logs in the **Event Log List** window. All event logs will be erased when you select **Clear All Logs** option. Select the **Clear Log Precede Index: X** option will erase the events that range from the beginning to the one you selected.

Configuration List Window

Every detail of the RAID system is presented in the Configuration List window. The information includes system information, controller settings, logical drive setting(s), logical volumn setting(s), channel setting(s), host

LUN list, drive-side parameters, caching parameters, and communication information.



Right-click on the Configuration List window will allow you to select four (4) options and they are explained as follow:

Export Configuration Data as Text File: When you select this option, the program will save the system's configuration data to a text file. You may select a file destination in a prompt up **Save** window.

Export Configuration Data as XML File: Select a file location where you like to save the system's configuration data as an XML file in a prompt up **Save** window when you select this option.

Export Host LUN List as XML File: This option will only export Host LUN list to an XML file. You may select a file destination in a **Save** window.

Restore Configuration from XML File: You may retrieve the configuration data that you exported earlier to the system. Select a file you previously saved from the **Open** window.

11.3 Logical Drive Information

Logical Drive Information helps you to identify the physical locations and logical relationship among disk drive members. In a massive storage application, a logical array may consist of disk drives installed in different drive enclosures.

The Logical Drive information is designed for today's complicated configurations of RAID arrays. The information window helps to achieve the following:

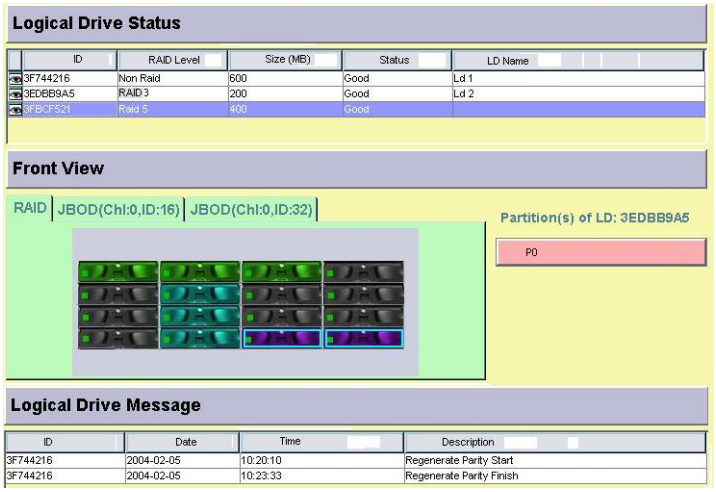
- Having a clear idea of the logical relationship can help avoid removing the wrong drive in the event of drive failure. A logical drive (RAID) configuration of disk drives cannot afford two failed disk drives.

- A logical drive may include members that reside on different enclosures or different drive channels. Doing so can help reduce the chance of downtime if a hardware failure should occur.

- With operations such as manual rebuild or capacity expansion using the "Copy and Replace" methodology, it is crucial to correctly identify an original member (source drive) and a replacement drive.

Accessing Logical Drive Information

Step 1. To access the **Logical Drive Information**, single-click its display icon on the GUI navigation panel or select the command from the **Action** command menu. After opening the information window, select the logical drive with a single mouse-click. A display window as shown below will appear.



Step 2. As shown above, once a configured array is selected, its members will be displayed as highlighted drive trays in the Front View window. The array's logical partition is displayed on the right. Each logical configuration of drives is displayed in a different color. If a selected array includes members on different enclosures, click the JBOD tab button on top of the enclosure graphic to locate their positions.

NOTE:

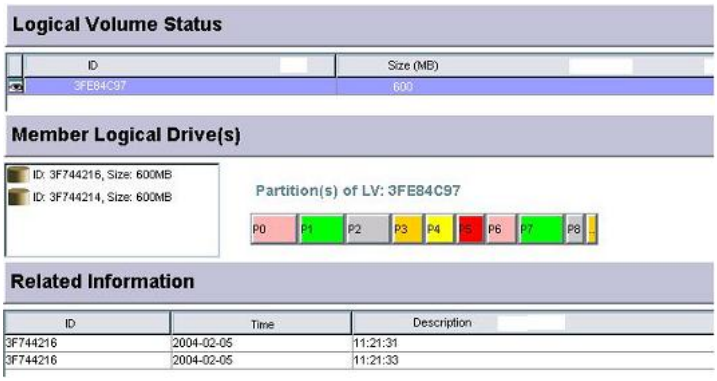
The **Logical Drive Messages** column only displays messages that are related to a selected array.

11.4 Logical Volume Information

A logical volume consists of one or many logical drives. Data written onto the logical volume is striped across the members.

Accessing Logical Volume Information

Step 1. To access the **Logical Volume Information**, single-click its display icon on the navigation panel or select the command from the ***Action*** command menu. After opening the information window, select a logical volume by single mouse-click. The window defaults to the first volume on the list.



Step 2. As shown above, once a configured volume is selected, its members will be displayed in the Members column. The volume's logical partition(s) are displayed on the right as a segmented color bar. Each segment represents a partition of the volume capacity.

NOTE:

The **Related Information** column only displays messages that are related to the selected volume.

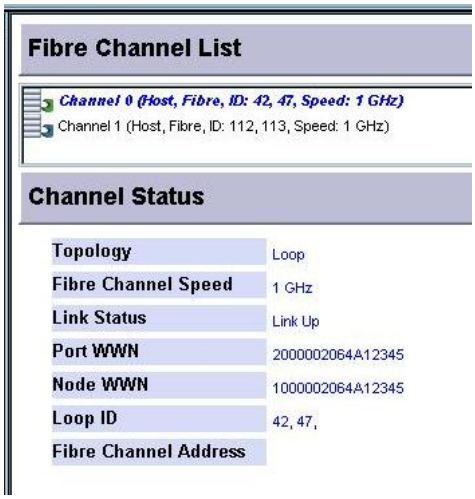
11.5 Fibre Channel Status

This window is automatically grayed out on subsystems featuring SCSI or iSCSI host channels. The Fibre Channel Status window displays information such as WWN port name and node name. This information is necessary in storage applications managed by SAN management software or failover drivers.

Step 1. To access the window, click on the **Fibre Channel Status** icon on the GUI navigation panel or select the command from the **Action** command menu.

The events in the window are listed according to the date and time they occurred with the most recent event at the bottom. A description of each event is provided.

Step 2. A Refresh button allows you to renew the information in cases when loop IDs are changed or an LIP has been issued.



11.6 System Information

This is a view-only window. This window contains information about the operating status of major components including CPU, board temperature, and enclosure modules like cooling fan and power supply units.

If the application includes multiple cascaded enclosures, you may also refer to the Enclosure View window where a faulty unit is indicated by the lit red LED. The color display of the LEDs shown on enclosure graphics corresponds to the real situation on the enclosure modules.

System Information

Device Name	Value	Status
CPU Type	PPC750	
Total Cache Size	512MB(ECC SDRAM)	
Firmware Version	3.34A	
Bootrecord Version	1.31K	
Serial Number	3460402	
Power Supply 1		Power supply functioning normally
Power Supply 2		Power supply functioning normally
Fan 1	8766.0 RPM	Fan functioning normally
Fan 2	8437.0 RPM	Fan functioning normally
Fan 3	8544.0 RPM	Fan functioning normally
Fan 4	8766.0 RPM	Fan functioning normally
CPU Temp Sensor	53.5 C	Temp. within safe range
Board1 Temp Sensor	50.0 C	Temp. within safe range
Board2 Temp Sensor	64.0 C	Temp. within safe range
+3.3V Value	3.336 V	Voltage within acceptable range
+5V Value	5.072 V	Voltage within acceptable range
+12V Value	12.199 V	Voltage within acceptable range
Battery-Backup Battery		Battery charging OFF(battery fully charged)
Power Supply 0		Power supply functioning normally
Power Supply 1		Power supply functioning normally
Fan 0	6.0 RPM	Fan functioning normally
Fan 1	6.0 RPM	Fan functioning normally
Fan 2	6.0 RPM	Fan functioning normally
Fan 3	6.0 RPM	Fan functioning normally
Temperature Sensor 0	27.0 C	Temp. within safe range
Device Slot 1		Slot is empty
Device Slot 2		Slot is empty

Step 1. To access the window, click on the **System Information** icon on the GUI navigation panel or select the command from the **Action** command menu.

Step 2. Carefully check the display icons in front of the Device Name. Devices are categorized by the data bus by which they are connected. See the icon list below for more information:

Icon	Description
	RAID controller status
	Status of I^2C bus devices
	Status of SAF-TE devices
	Status of SES devices
	Temperature sensors

Table 11-3: Device Icon

A Refresh button allows you to renew the information in cases when loop IDs are changed or when an LIP has been issued.

NOTE:

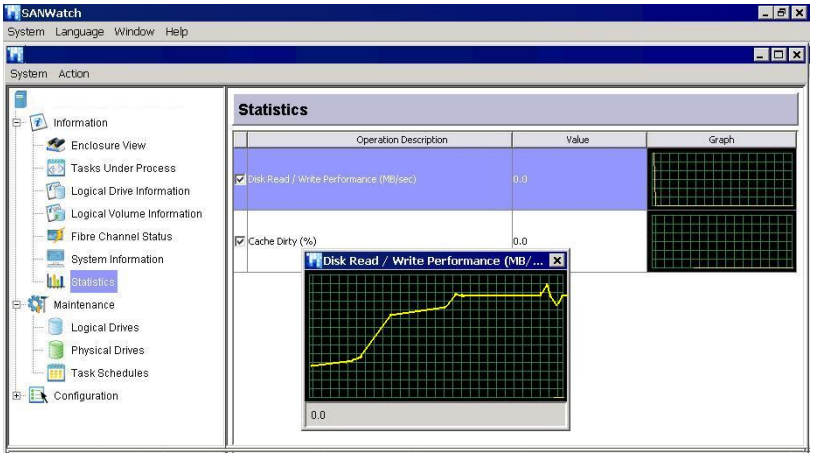
Place your cursor on a specific item to display its device category.

Component status is constantly refreshed, yet the refresh time depends on the value set for device bus polling intervals, e.g., polling period set for SAF-TE or SES devices.

The EonStor subsystem series supports auto-polling of cascaded enclosures, meaning the status of a connected enclosure is automatically added to the System Information window without the user's intervention.

11.1 Statistics

SANWatch Manager includes a statistics-monitoring feature to report the overall performance of the disk array system. This feature provides a continually updated real-time report on the current throughput of the system, displaying the number of bytes being read and written per second, and the percentage of data access being cached in memory. These values are displayed by numeric value and as a graph.



To access the Statistics window, click on the **Statistics** icon on the GUI navigation panel or select the **Statistics** command from the **Action** menu. Then choose either **Cache Dirty (%)** or **Disk Read/Write Performance (MB/s)** by checking the respective select box.

- The **Cache Dirty** statistics window displays what percentage of data is being accessed via cache memory.

- The **Read/Write Performance** window displays the amount of data being read from or written to the disk array system, in MB per second.

This page is intentionally left blank.

Chapter 12
Enclosure Display

This chapter introduces the enclosure display using the Enclosure View window in the SANWatch's main program.

- **About The Enclosure View – Section 12.1**
- **Accessing the Enclosure View – Section 12.3**
  - **12.2.1 Connecting to the RAID Agent**
  - **12.2.2 Opening the Enclosure View Window**
  - **12.2.3 Component Information**
- **LED Representations – Section 12.3**
- **Enclosure View Messages – Section 12.4**
- **Information Summary – Section 12.5**

12.1 About The Enclosure View Window

The SANWatch Enclosure View is a customized display that shows a visual representation of the physical RAID controller/subsystem components. The Enclosure View allows you to quickly determine the operational status of critical RAID components.

The Enclosure View window shows both the front and rear panel (e.g., the EonRAID 2510FS controller head series, see ***Figure 12-1***). The Enclosure View of each SANWatch session defaults to the display of the connected RAID controller or RAID subsystem. The tabbed panel provides access to other cascaded enclosures (e.g., JBODs, the EonStor series, see ***Figure 12-2***), so you can monitor multiple enclosures via a single SANWatch management session.

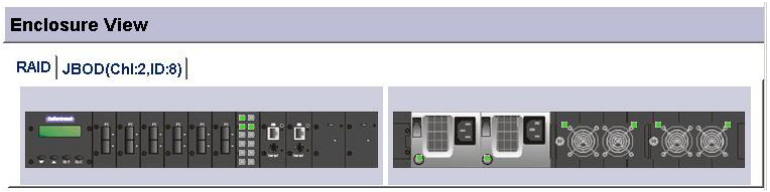


Figure 12-1: EonRAID 2510FS Enclosure View

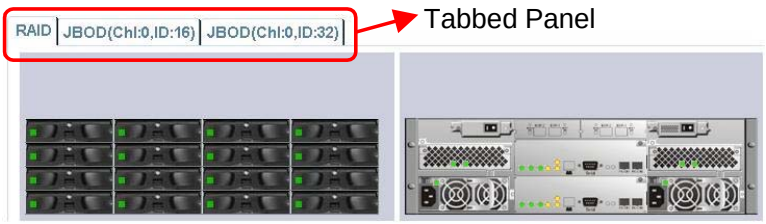


Figure 12-2: EonStor F16F Series Enclosure View

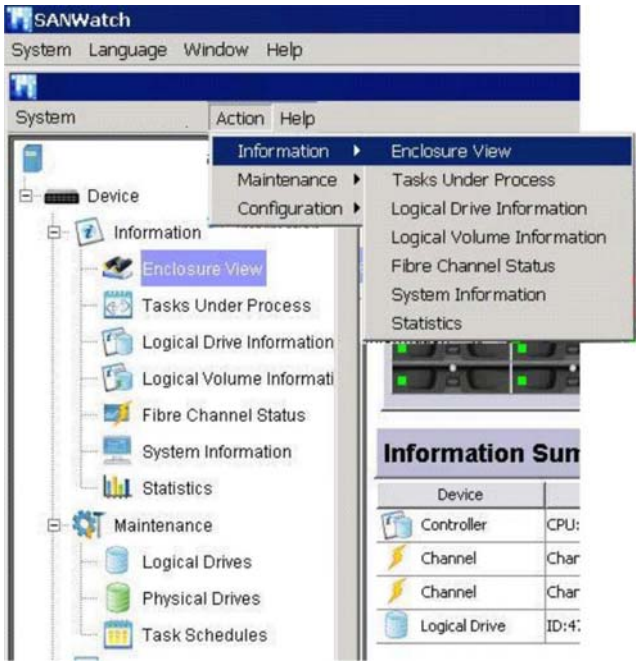
12.2 Accessing the Enclosure View

12.2.1 Connecting to the RAID Agent

Connection to the RAID Agent is fully described in ***Chapter 3*** of this manual.

12.2.2 Opening the Enclosure View Window

Once SANWatch is successfully connected to a RAID subsystem, SANWatch defaults to the Enclosure View. If it doesn't appear or if you have closed the Enclosure View window but wish to access it again, you can either select the Enclosure View icon from the navigation tree or go to the Action Command menus and then select Information/Enclosure View on the top of the screen.



12.2.3 Component Information

The front and rear views of a RAID subsystem in the Enclosure View window are the exact representations of physical components. This window is particularly useful in monitoring the status of the physical drives. It provides a real-time report on the drive status, using LED colors to represent various operating statuses.

The Enclosure View displays information about the following RAID components:

- **RAID Controller** – The RAID controller is the heart of any RAID enclosure and controls the flow of data to and from the storage devices.

- **I/O Channels** – An I/O channel is the channel through which data flows to and from the RAID controller.

- **Battery Backup Unit (BBU)** – The BBU provides power to the memory cache when power outage occurs or the power supply units fail.

NOTE:

The BBU is an optional item for some subsystem models.

- **Power Supply Unit (PSU)** – All RAID devices should come with at least one PSU that provides power to the RAID device from the main power source.

- **Cooling Module** – All RAID devices should come with at least one cooling module.

12.3 LED Representations

As described earlier (see ***Section 12.1***), the Enclosure View is a direct representation of the physical devices. Almost every major component has its status-indicating LEDs. When a component fails (or some other event occurs), the related LEDs will flash or change the display color. The physical status of the LEDs will be reflected by the LEDs shown in the **Enclosure View** window. That is, if an LED on the physical device changes its display color, then the display color of the corresponding LED in the Enclosure View window will also change.

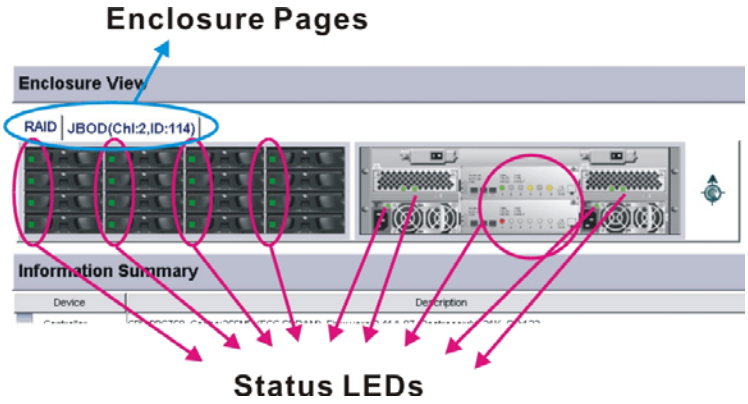


Figure 12-3: Enclosure Tabbed Panel and Component LED Display

The definition for each LED has been completely described in the ***Installation and Hardware Reference Manual*** that came with your RAID controller/subsystem. Please refer to the manual to determine what the different LEDs represent.

12.3.1 Service LED (on Models that Come with an LED panel)

Service LED for RAID/JBOD subsystems:

The service LED can be enabled by SANWatch management software from a remote site to identify which subsystem is being serviced. The corresponding subsystem LED will also be lighted in the SANWatch GUI.

Pressing the service button on the subsystem can also enable the service LED.

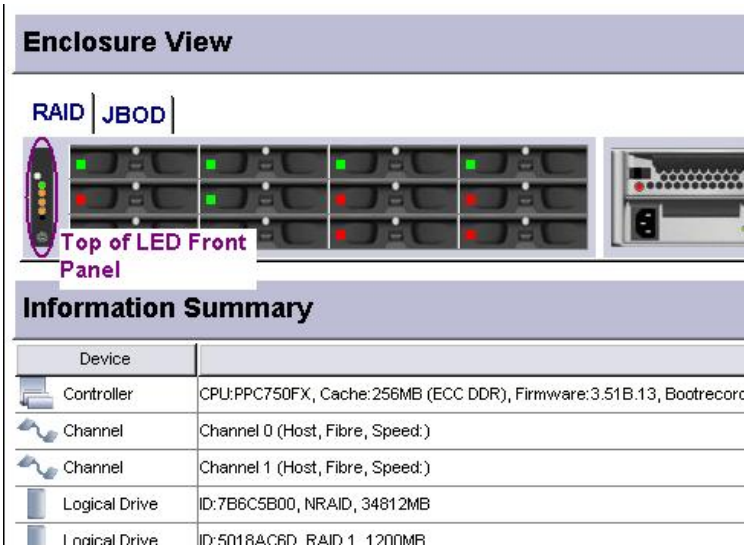


Figure 12-4: Service LEDs

After servicing the subsystem, the administrator should turn off this service LED by manually pressing the service button on the chassis or remotely using the SANWatch management software.

12.4 Enclosure View Messages

The messages shown in the Enclosure View window provide easy access to information about components of a RAID enclosure that is being monitored. The message tag reports the status of major devices.

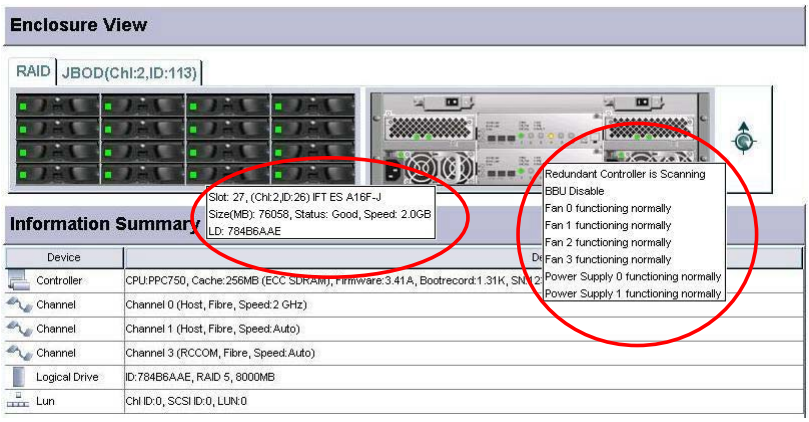


Figure 12-5: Component Information Message Tags

To generate the message tags, move the mouse cursor onto the relevant RAID device component. For example, if you wish to determine the operational status of a RAID subsystem, move the cursor onto the enclosure graphic and the corresponding message tag will appear.

The enclosure front view message tag displays the current configuration of the drive, including the channel number of the drive slot on the subsystem to which the drives are connected, the drive's capacity, transfer rate, and current status.

The enclosure components function as a summary of module operating status. The operating status of each module is shown either as operating normally or failed.

NOTE:

Messages do not always appear instantaneously. After the cursor has been moved onto the component, there is usually a delay of a second before the message tag appears.

NOTE:

More device-dependent information is provided in the System Information window. To access the System Information window, please refer to **Chapter 6**.

12.5 Information Summary

The Information Summary window displays key information on the subsystem currently selected, including the RAID controller(s), I/O channels, connection speeds, logical drive status, LUN mapping status…etc.

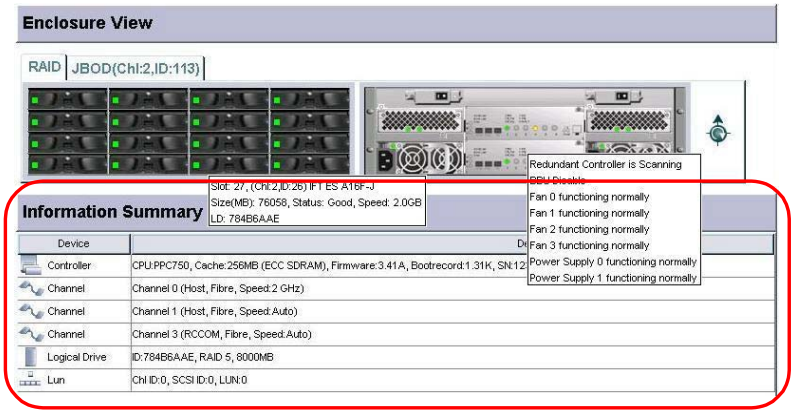


Figure 12-6: Information Summary

Chapter 13
NPC Utility Installation

This chapter introduces the NPC utility. The following topics are discussed:

- **The NPC Utility – Section 13.1**
  - **13.1.1 The NPC Utility**
  - **13.1.2 To Access the Utility**
- **Configuring the Utility Options – Section 13.2**
  - **13.2.1 SSL**
  - **13.2.2 Email Notification**
  - **13.2.3 SNMP Traps**
  - **13.2.4 Broadcast**

13.1. The NPC Utility

13.1.1 Introduction

NPC stands for "Notification Processing Center." This utility is used to deliver event messages when the main SANWatch modules are installed to a RAID subsystem's segregated disk capacity, the reserved space. NPC is implemented to manage event notification functions since the Configuration Client utility is not available with the Mode 3 installation scheme. With Mode 3 installation, arrays are accessed directly through network connections without installing the manager software and utilities onto a server. The NPC utility is automatically distributed to a disk array's reserved space when installing SANWatch using the Mode 3 installation scheme.

13.1.2 To Access the Utility

The NPC utility is easily accessed using a web browser over the network.

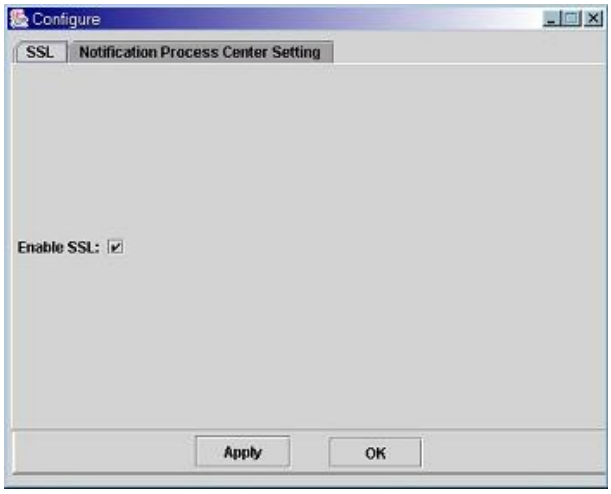
Step 1. Open a web browser program.

Step 2. Enter "**http://<controller IP>/configure.htm**" in the web browser's URL field.

Step 3. A safe content warning message might prompt. Click **Yes** to proceed. (See *Error! Reference source not found.*)

Warning - Security
Do you want to trust the signed applet distributed by "Infortrend Inc."?
Publisher authenticity verified by: "Infortrend Inc."
The security certificate was issued by a company that is not trusted.
The security certificate has not expired and is still valid.
Caution: "Infortrend Inc." asserts that this content is safe. You should only accept this content if you trust "Infortrend Inc." to make that assertion.
More Details
Yes
No
Always

Step 4. The configuration utility starts as a Java Applet.



13.2. Configuring the Utility Options

13.2.1 SSL

SSL stands for "Secure Sockets Layer Handshake Protocol." As shown above, the initial screen defaults to the SSL option. Select the check box if you want to enable SSL connection for the management session with the array.

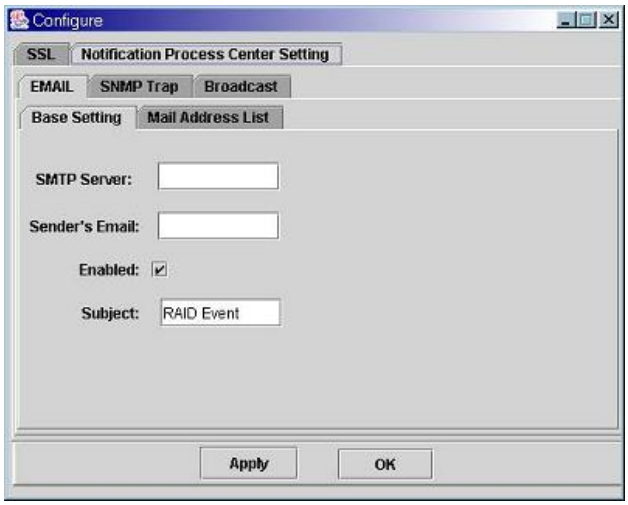
NOTE:

The configuration will take effect after you restart the network connection or reset the management station.

13.2.2 Email Notification

Follow the steps below to configure email notification:

Step 1. Click on the **Notification Process Center Setting** tab. Open the **Base Setting** page.



Step 2. Fill in or select the following configuration fields:

SMTP Server: The Internet mail server used to send event notification.

Sender's email: Enter a valid mail address, the "From" part of email notification functionality.

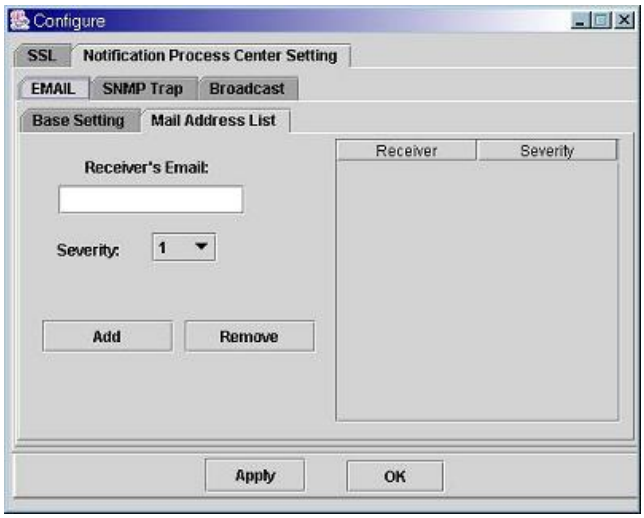
Enabled: Select this check box to enable email notification.

Subject: Allows you to append a subject matter to event notification emails; e.g., "Events from RAID 3 array."

Step 3. Click **Apply** or **OK** to proceed with configuration. Note that the configuration will be saved to the reserved space on the array and may cause a short delay.

Step 4. Click **Mail Address List** from the tabbed panel above.

Fill in or select the following configuration fields:



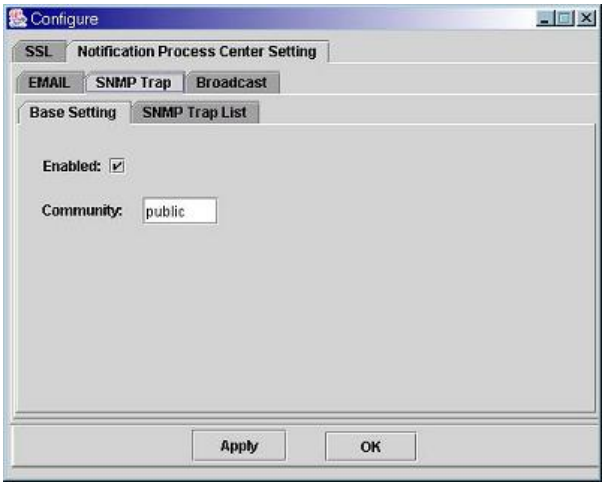
Receiver's email: Shows a list of all the email addresses that the NPC will send a message to. Addresses added will be listed on the right.

Severity: Select the severity level of events to be sent to the receiver station.

Step 5. Click **Apply** or **OK** to complete the configuration.

13.2.3 SNMP Traps

Step 1. Click on the **Notification Process Center Setting** tab and **SNMP Trap** to display SNMP settings.



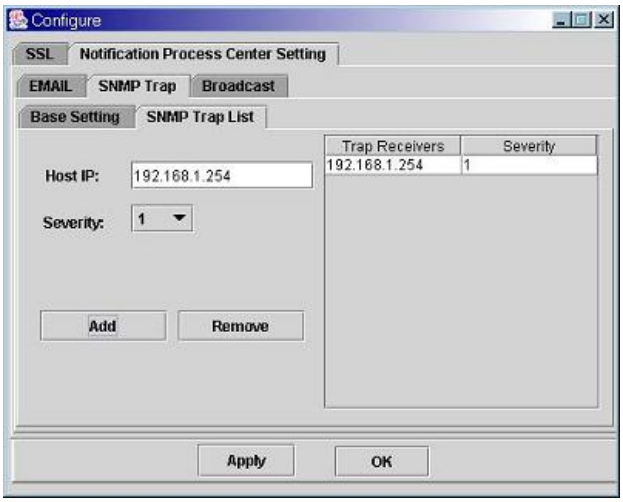
Step 2. Fill in or select the following configuration fields:

Enabled: Select this check box to enable the notification.

Community: This is just a string authentication and can be seen as a plain text password.

Step 3. Click **Apply** or **OK** to proceed with configuration. Note that the configuration will be saved to the reserved space on the array and may cause a short delay.

Step 4. Click **SNMP Trap List** from the tabbed panel above.



Host IP: The port number of the agents listening for traps.

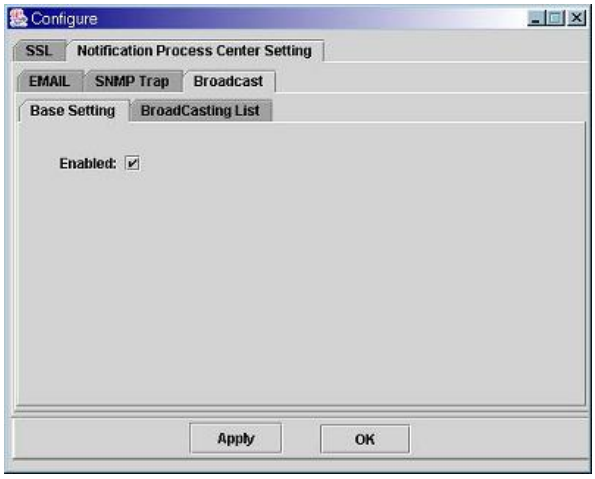
Severity: Select the severity level of events to be sent to the receiver station.

Trap receivers will be added to the **Trap Receivers** list on the right.

Step 5. Click **Apply** or **OK** to complete the configuration.

13.2.4 Broadcast Notification

Step 1. Click on the **Notification Process Center Setting** tab and **Broadcast** to display Broadcast settings.



Step 2. Fill in or select the following configuration fields:

Enabled: Select this check box to enable the notification.

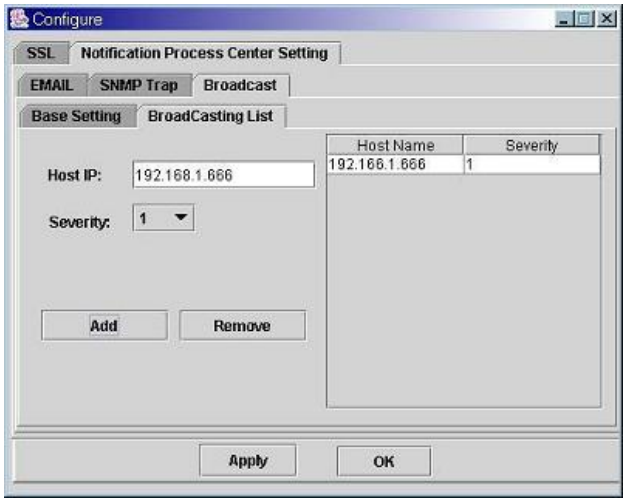
Step 3. Click **Apply** or **OK** to proceed with configuration. Note that the configuration will be saved to the reserved space on the array and may cause a short delay.

Step 4. Click **Broadcasting List** from the tabbed panel above.

Host IP: The IP address a broadcast message will be sent to.

Severity: Select the severity level of events to be sent to the receiver station.

Computers receiving broadcast messages will be added to the Host Name list on the right.



Step 5. Click **Apply** or **OK** to complete the configuration.

IMPORTANT!

In a massive capacity configuration, it takes a while for the RAID subsystem to write the NPC configuration profile to every disk member. DO NOT reset or power down the subsystem before the configuration can be safely distributed to the array.

Also make sure the subsystem's Ethernet port and related TCP/IP settings have been properly configured for the NPC functionality to take effect.

Chapter 14
Central Management Utility

This chapter introduces the Centralized Management utility. The following topics are discussed:

- **Centralized Management Section 14.1, page 14-2**
- **Setting Up the Utility Section 14.2, page 14-2**
- **Central Management Connection Section 14.3, page 14-4**
- **Maintenance & Configuration Section 14.4, page 14-4**
  - **14.4.1 Icon Labels**
  - **14.4.2 System Events**

14.1. Centralized Management Introduction

The Centralized Management utility provides:

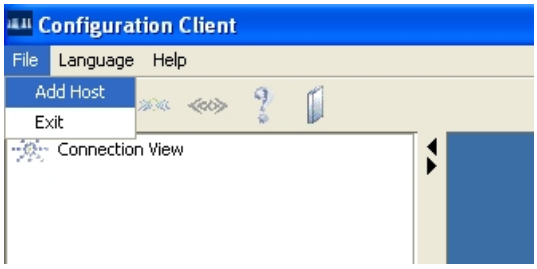
- Online monitoring of Infortrend RAID subsystems over the network
- Creation of instant event logs
- Filtering and exporting event logs via text files

The Centralized Management utility is an entrance portal to SANWatch whereby you can configure and maintain subsystems. Simply click the icon to connect to the subsystem.

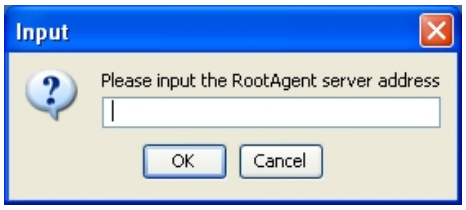
14.2. Setting Up the Utility

The **Central Management** utility, along with the **Configuration Client** and SANWatch, can be accessed through the shortcut the icons on your desktop or traditionally through the Start menu.

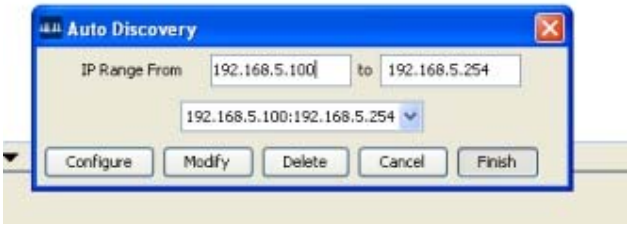
Step 1. Open the **Configuration Client** and select **Add Host**.



Step 2. Add one (1) **Root Agent** by entering the IP address (the IP address of the management station where you installed the Configuration Client) for the Root Agent.



Step 3. Select the **Auto Discovery** option from the **Module Name** drop-down box.



Step 4. Define the IP scan range to search the network. Click *Finish*.

Step 5. Double-click the ON/OFF switch.

The Root Agent will automatically scan the IP range for available subsystems on the network.

Step 6. Check the scan results in **RootAgent Setting**.

IMPORTANT!

The **Auto Discovery Module** only supports the Firmware versions listed below.

FW 3.42H03 or later - Fibre to SATA
FW 3.42J09 or later - SCSI to SATA
FW3.42R01 or later - Fibre to Fibre

Auto Discovery cannot detect a subsystem if the firmware version is older then those listed above. However, you can still manually provide the subsystem's Agent IP.

14.3. Central Management Connection

The **Central Management** utility displays system information via the intermediate Root Agents. The information is queried indirectly from the Root Agents that in turn acquire system information from their subordinate RAID subsystems. The connections with these agents are displayed using colorful icons.

Figure 14-1: Not Connected

The above icon shows a failed connection window.

Figure 14-2: Data Query

The above icon shows that the Central Management utility is querying data from the Root Agent.

Figure 14-3: Connected

The above icon shows that the Central Management utility is connected with the Root Agent.

Figure 14-4: Connecting

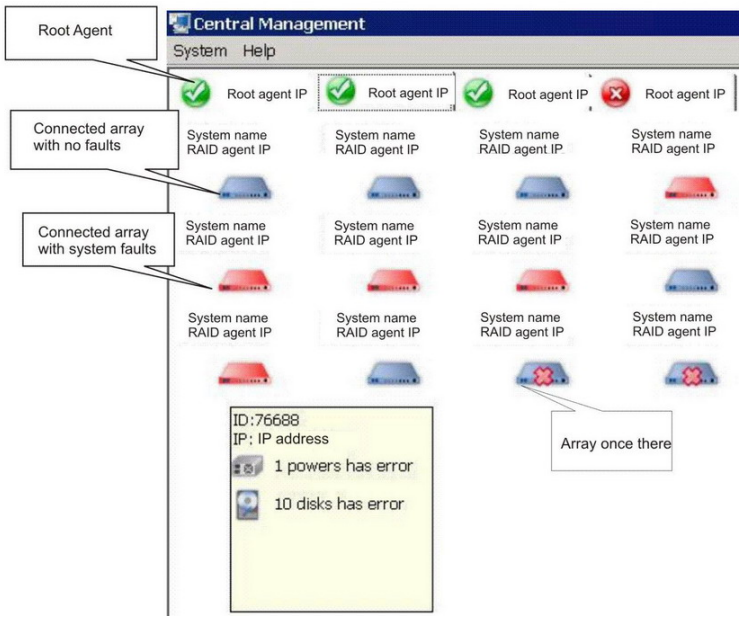
The above icon shows that Centralized Management is still trying to connect with a Root Agent.

14.4. Maintenance & Configuration

14.4.1 Icon Labels

Icon labels display the model name and the IP address of the connected RAID subsystems.

Single-click on a Root Agent, and then its subordinate RAID systems will appear. Move the cursor over the subsystem icon and an information box will pop up with detailed information such as, the System Name, ID, IP address, and the number of component or RAID configuration events.



NOTE:

The red icons indicate the arrays with the occurrences of system faults or warning messages. Icons with a cross mark are those that can not be accessed. Please check whether the subsystems are powered down, its network link fails, or its IPs have been changed.

14.4.2 System Events

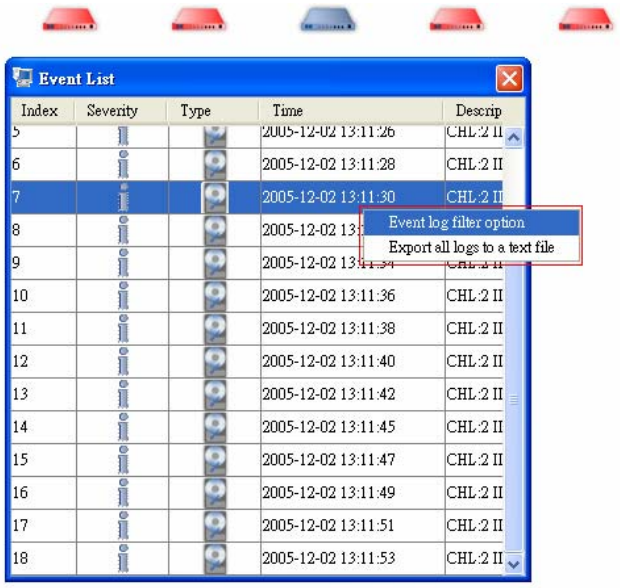
A single click on an array icon displays two (2) options:

Connecting the RAID subsystems

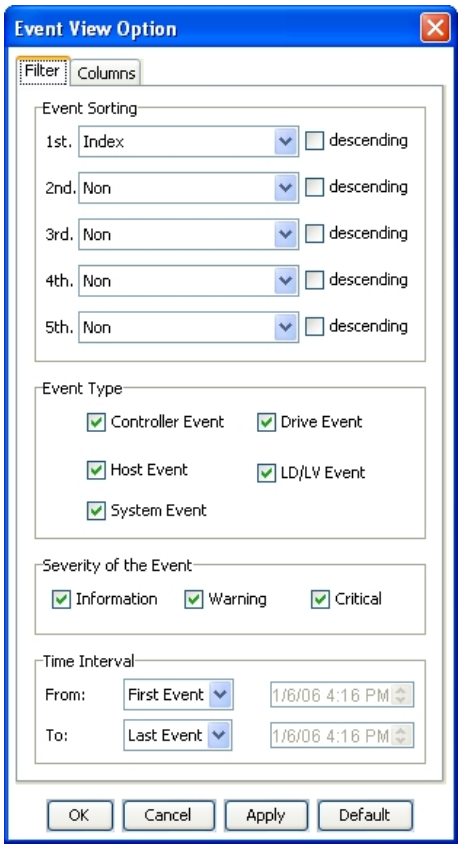
1. A single click on the "**Connect**" command establishes a SANWatch console with the RAID subsystem.

2. A single click on the "**Event log**" command displays a list of system events.

Filter and export log

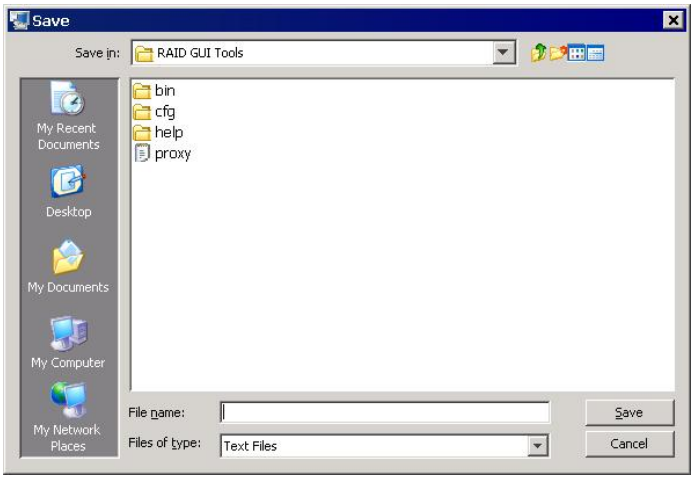


3. A right-click on the event list displays two (2) event log-related options – the "**Event Log Filter**" and the "**Event Export**" commands.



The **Event log filter option** allows you to filter events based on various criteria. The same functionality can also be found in SANWatch's system view window.

The **Event Export** command allows you to save the event list as a simple text file to your system drive. Shown below is a Windows prompt. Enter a file name and save the event log as a text file.



This page is intentionally left blank.

Chapter 15

Data Service: Snapshot

This chapter introduces the beginning of data service functionalities, the snapshot function group. Topics include:

- **Snapshot Basics**
- **Configuration Process**
- **Snapshot Purge Policy (Space Management)**
- **Snapshot Scheduler & Prune Policy Configuration**

15.1 Snapshot Basics

One of the difficulties of performing backup or retrieving data for other uses is that users' access to the source data volume has to be temporarily stopped. Traditionally, this could be accomplished by going to a backup in a tape library. However, retrieving data from tapes may take hours, days, or even weeks. There are alternatives such as mirrored volumes; but, producing full synchronization of two operating volumes consumes enormous resources and disk space.

Infortrend's snapshot is developed from a widely-applied point-in-time and copy-on-write methodology. A sequence of snapshot actions through a time line is described and diagrammed as follows:

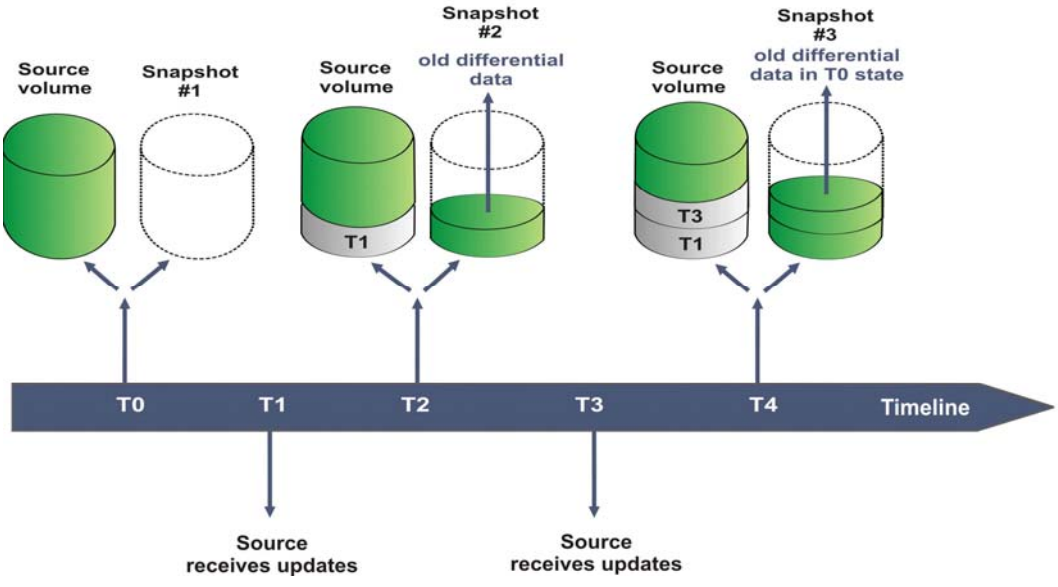


Figure 15-1: Snapshots through a Time Line

Actions on the Time Line:

T0: A snapshot image of source volume is taken at T0. At T0, the snapshot volume is actually empty except for a tag and a time table.

T1: At T1, the source volume receives updates from host.

T2: At T2, the RAID firmware generates and distributes block-level differentials of the data that is to be overwritten by the T1 updates to the snapshot image.

T3: Source volume receives another update.

T4: Firmware generates and distributes differentials of the data that will be overwritten by the T3 updates to the snapshot image.

In this way, snapshot keeps the update history as the snapshot image of the source volume at its T0 state.

Snapshot only maintains update history and data block differentials, and thereby consumes very little storage space.

Snapshot Uses:

Applications: Data backup, data analysis and reporting, testing & research, database recovery.

Benefits: Faster Backup – Snapshot helps you quickly backup data at any time. Backup copies can be created from snapshot images, thus eliminating the needs to stop host I/Os. Backup jobs can be processed with little impact to file serving performance.

In general, Snapshot is many times faster than traditional tape or software backup and is driven by RAID system hardware meaning the operation consumes no resources on the application servers.

Access:

If the need arises for access to individual files at its T0 state, those specific data files will be regenerated by comparing the differentials in snapshot images and data in the source volume. Data can be retrieved without affecting normal access to the source volume.

By mapping a Snapshot Image to a host LUN, you can access the original source volume at a specified point in time.

Snapshot Image Repository:

Infortrend snapshot uses additional LUNs (RAID volumes) to keep snapshot configuration profiles and block-level differentials.

Snapshot Hierarchy:

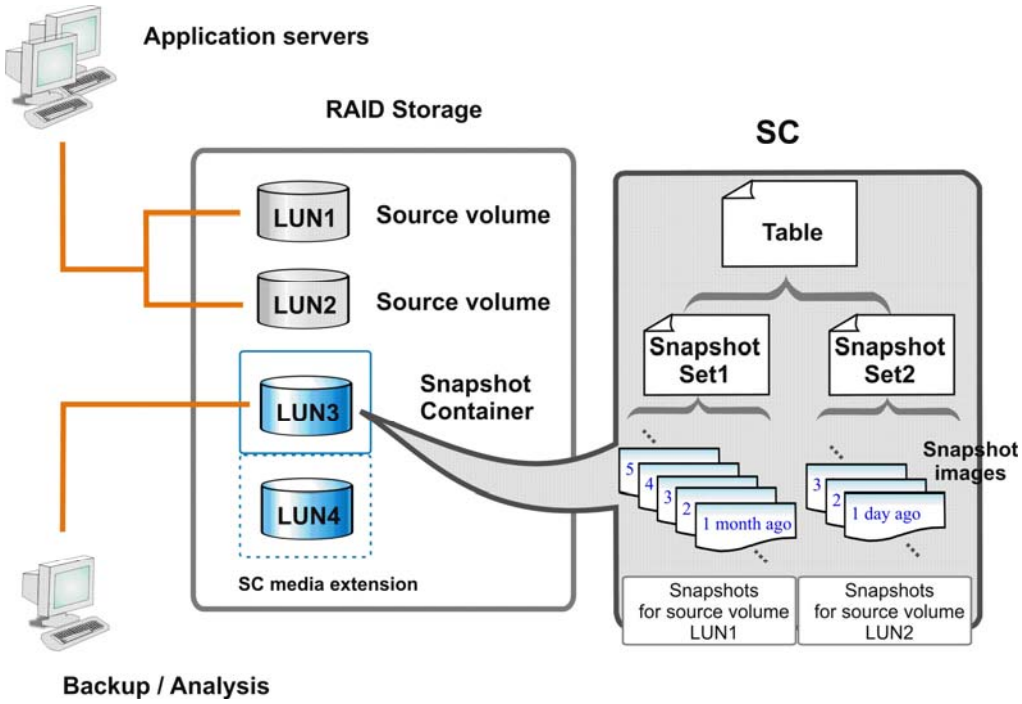


Figure 15-2: Snapshot Relevant Directory Architecture

Snapshot Container (**SC**):

A reserved space allocated for saving all snapshot configurations and subordinate directories referring to one or several source (production) volumes.

Snapshot Set (**SS**):

Directories that contain snapshot related information for a specific source volume.

Snapshot Image (**SI**):

Snapshot images keep block-level differentials of the data overwritten by host writes since the time a snapshot was taken for a specific source volume.

Snapshot Maintenance

Snapshots should be properly managed for the optimal use of disk space and backup efficiency. Various commands, Purge & Prune policies are available for maintaining efficient snapshot directories by removing outdated images, configuration, and/or acquiring more snapshot space by expanding an existing Snapshot Container:

- Snapshot Container – **Create**, **View**, **Recovery**, **Delete**, **Expand**, **Set Space Threshold**
- Snapshot Set – **Create**, **View**, **Recovery**, **Delete**, **Purge Policy**, **Delete Policy, Map to Host**
- Snapshot Image – **Create**, **View**, **Delete**, **Map to Host**
- Snapshot Volume Expansion - Snapshot Containers can be expanded by joining in another RAID volume, e.g., a partition of a

logical drive. After a period of time, you may gradually use up the storage space allocated for the container volume. If you have unused disk space (an independent array or logical partition), you may combine the space with an existing Snapshot Container.

15.2 Configuration Process

Using the SANWatch: License Login

IMPORTANT!

A Profession version of 30-day trail is available without downloading the license key. See the following section for how to activate the trial use.

A licensed login requires:

1. At least a 512MB cache in your RAID subsystem.
2. Purchasing SANWatch by the following license application procedure.
3. A corresponding firmware version with the support for functionalities such as snapshot.

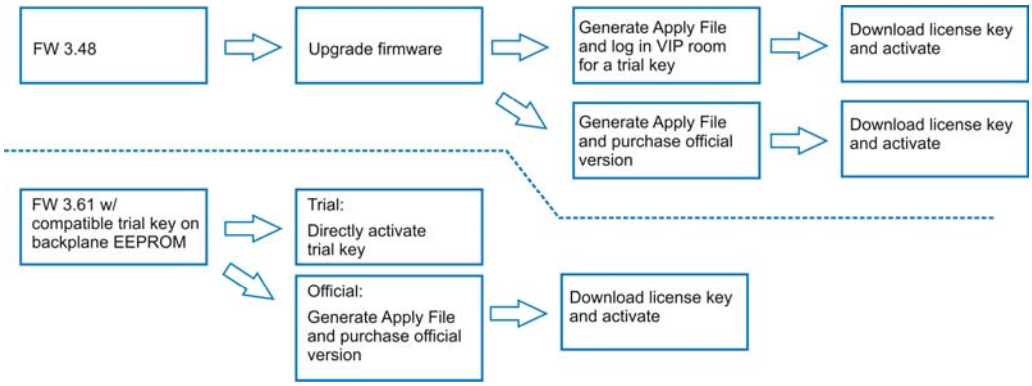

FW 3.48
Upgrade firmware
Generate Apply File and log in VIP room for a trial key
Download license key and activate
Generate Apply File and purchase official version
Download license key and activate
FW 3.61 w/ compatible trial key on backplane EEPROM
Trial:
Directly activate trial key
Official:
Generate Apply File and purchase official version
Download license key and activate

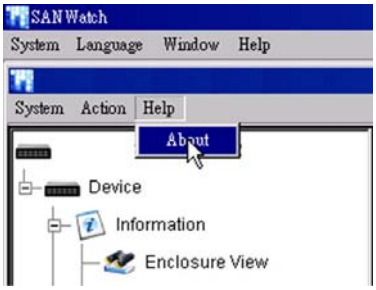
Figure 15-3: License Key Application Procedure Flowchart

The Trial Use Alternatives:

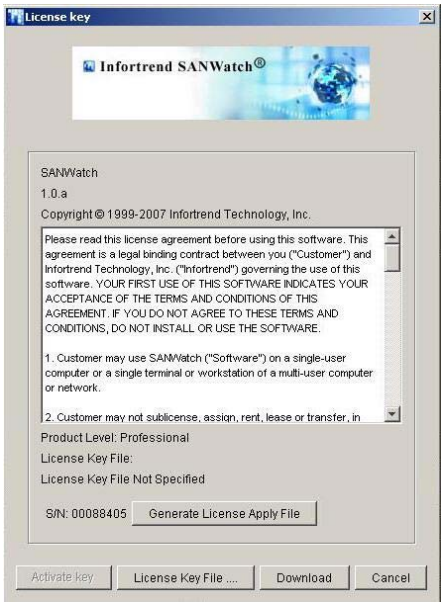
1. The Data Service functionality is enabled on a per enclosure basis. With older firmware, e.g., 3.48, you should proceed with the following:

   1-1. Upgrade firmware.

   1-2. Click on the **About** button on the **Help** menu of the array management window (not the outer shell window).



1-3. Generate a **License Apply File** by the clicking the button in the **License Key** window.


License key
Infortrend SANWatch
SANWatch
1.0.a
Copyright © 1999-2007 Infortrend Technology, Inc.
Please read this license agreement before using this software. This agreement is a legal binding contract between you ("Customer") and Infortrend Technology, Inc. ("Infortrend") governing the use of this software. YOUR FIRST USE OF THIS SOFTWARE INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT INSTALL OR USE THE SOFTWARE.
1. Customer may use SANWatch ("Software") on a single-user computer or a single terminal or workstation of a multi-user computer or network.
2. Customer may not sublicense, assign, rent, lease or transfer, in
Product Level: Professional
License Key File:
License Key File Not Specified
S/N: 00088405
Generate License Apply File
Activate key
License Key File ....
Download
Cancel

1-4. Send the Apply File to your vendor or log in our VIP room website to apply for a trial use. You can also directly purchase an official version of Data Service.

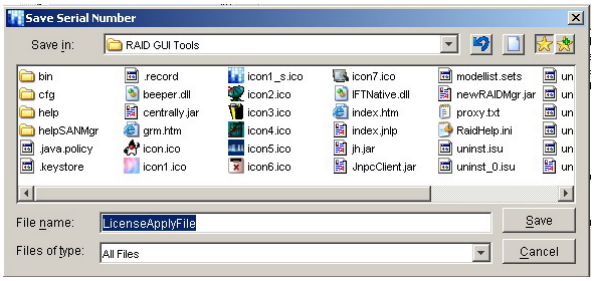
2. For a system that comes with SANWatch-compatible firmware (e.g., FW3.61), click on the **Activate key** button to begin the trial use.

If you do not want to activate this time, click the **Cancel** button.

Purchasing and Activating the License Key:

When the software is attempting access to a specific RAID system, the EEPROM serial number (**S/N**) is acquired as shown in the License Key window above. If not, you may need to upgrade firmware to a SANWatch-compatible version.

Step 1. To purchase the software, click on the "**Generate License Apply File**" button, a "**Save Serial Number**" window appears. Save the file to a preferred location.



Step 2. Send the Apply File to your vendor.

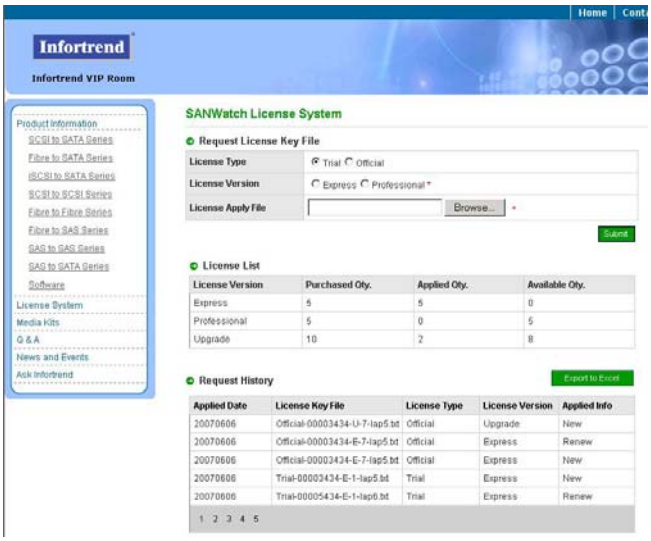
- OR -

If you are a certified vendor and you have a pre-paid account, visit our VIP room website (http://viproom.infortrend.com) to apply for a trial use or complete the purchasing process.

Log in using your VIP room user name and provide the password.

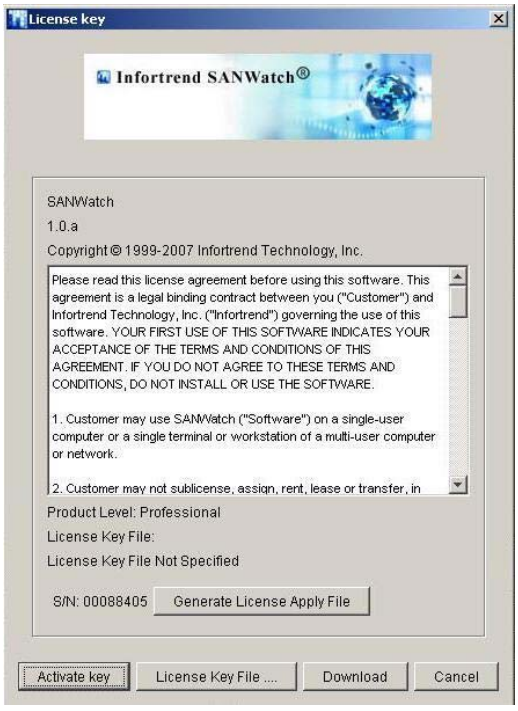
Click on **License System** to display the SANWatch registration window.

A **SANWatch License System** View will display. Upload your Apply File. When finished processing your request, we will deliver a **License Key File**.

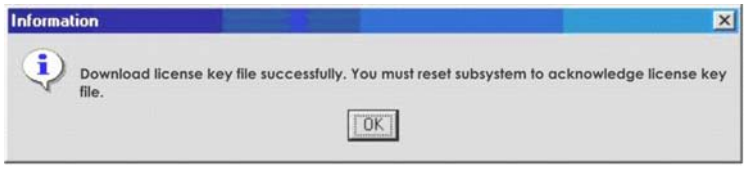


Step 3. Once you receive the License key file, use the **License Key File…** button to locate the file and use the **Download** button to update the corresponding firmware settings.

Step 4. Once firmware is successfully updated, the "**Activate Key**" button is enabled. Press the button to enable the licensed use of the software.


License key
Infortrend SANWatch®
SANWatch
1.0.a
Copyright © 1999-2007 Infortrend Technology, Inc.
Please read this license agreement before using this software. This agreement is a legal binding contract between you ("Customer") and Infortrend Technology, Inc. ("Infortrend") governing the use of this software. YOUR FIRST USE OF THIS SOFTWARE INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, DO NOT INSTALL OR USE THE SOFTWARE.
1. Customer may use SANWatch ("Software") on a single-user computer or a single terminal or workstation of a multi-user computer or network.
2. Customer may not sublicense, assign, rent, lease or transfer, in
Product Level: Professional
License Key File:
License Key File Not Specified
S/N: 00088405
Generate License Apply File
Activate key
License Key File ....
Download
Cancel

Step 5. You should then reset your RAID subsystem in order for the configuration change to take effect.



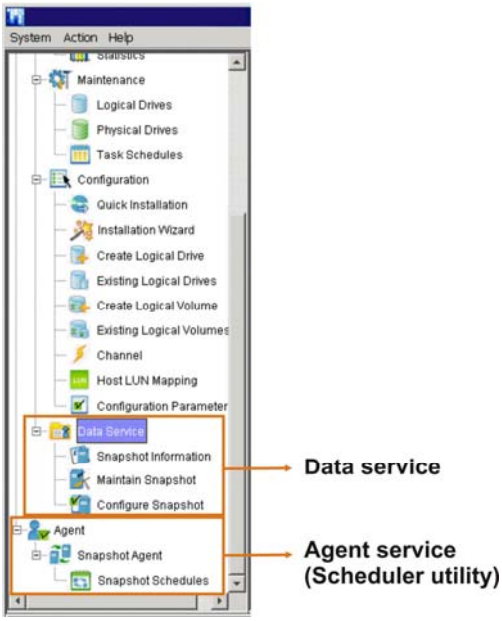
NOTE:

The optimal configuration for running the **Data Service** functionality in SANWatch is listed below:

RAID controller **caching mode**: write-back
Disk buffer: disabled
BBU protection: enabled
BBU **Event–triggered operation**: enabled

If your current firmware configuration does not match the above, when you activate the Data Service the above preferences will automatically apply.

GUI Structure



Snapshot options are categorized under the **Data Service** and the **Agent** function groups.

A single click on one of the function icons opens one of the following windows.

IMPORTANT!

The **Agent** function group appears only with an in-band, directly-attached connection. With flush agents running on host, OS/application caches can be properly flushed before taking snapshots; and therefore the Snapshot scheduler utility is only available where SANWatch is installed on a server that is directly attached to RAID storage.

A remote SANWatch console is also available by connecting the server IP, the RAID agents running on the application server act as flush agents as well as the bridging element between RAID system firmware and the management interface.

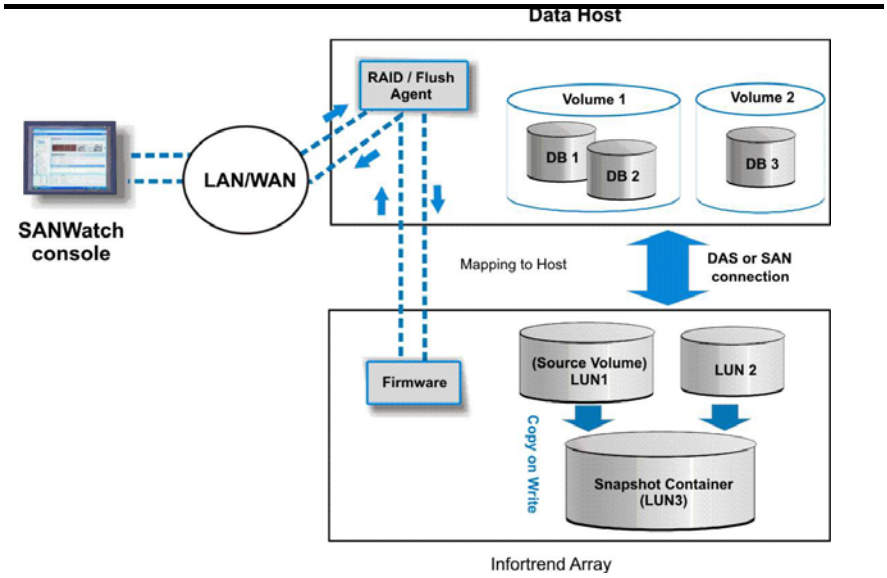
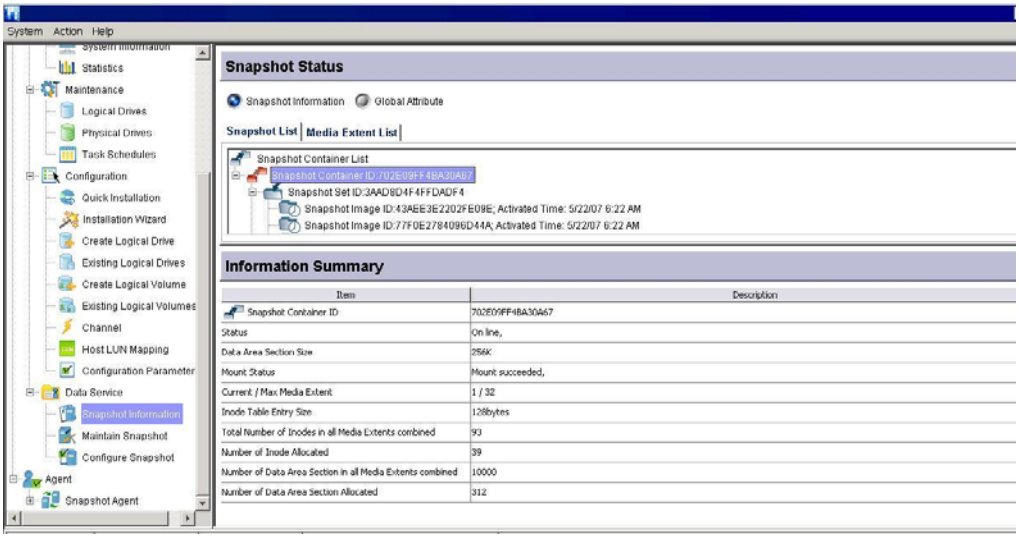
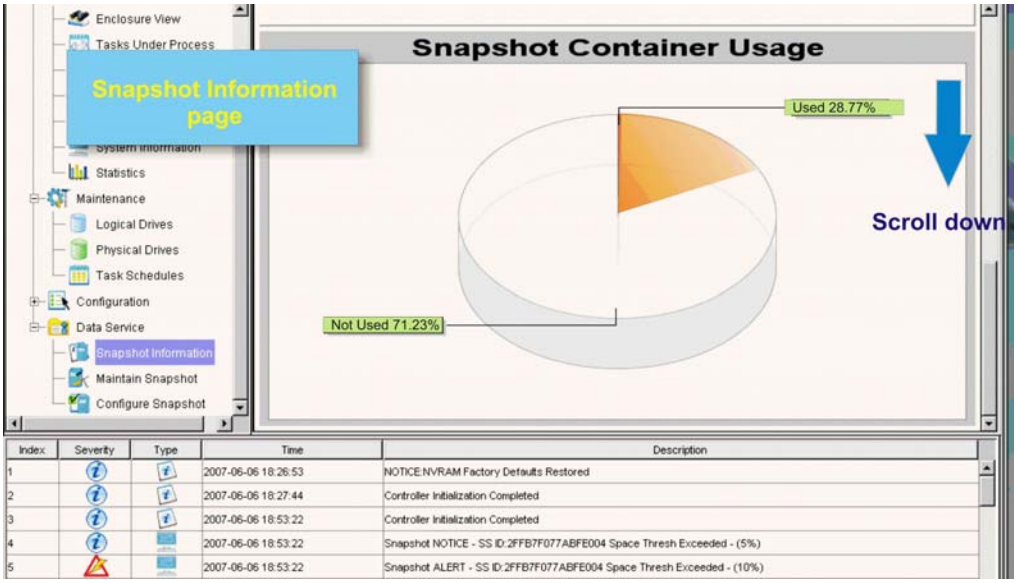


Figure 15-4: The Intermediate RAID Agents on a Direct-attached Server

Snapshot Information: provides access to the information of existing Snapshot Containers, Media Extent List, its subordinate Snapshot Sets and Snapshot Images.



Snapshot Space Usage Indicator: Scroll down on the Snapshot Status screen to see a percentage graph showing how much of storage space has been taken by snapshot images.

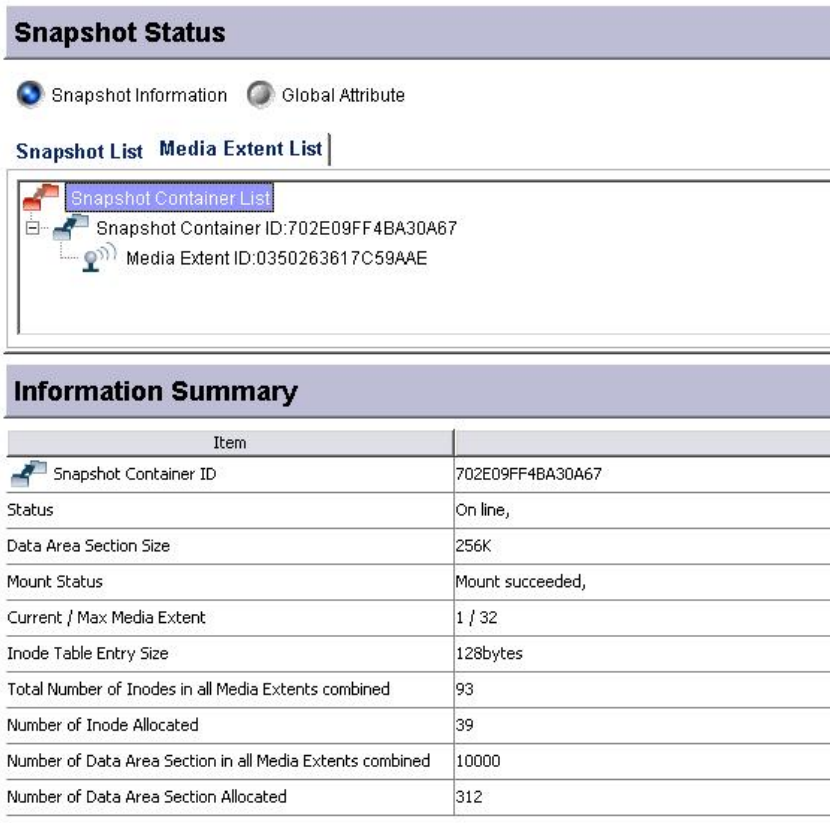


Screen Item Description:

Snapshot Container	
Snapshot Container ID	A randomly generated identifier for each Snapshot Container.
Online/Offline	The status of the Snapshot Container. Online means a valid SC configuration. Offline refers to states such as logical drive failure.
Data Area Section Size	The size of smallest allocation unit in snapshot data differentials. Similar to data blocks in ordinary storage media.
Mount Status	Array status (Status of the Source Volume that this Snapshot Container is referring to).
Current/Max. Media Extent	The number of RAID volume (LD, LV, or partitions) currently contained within this Snapshot Container and the max. number of volumes allowed.
Inode Table Entry Size	Inode refers to the infrastructure table used to organize data differentials, differential locations, and relational information
Total Number of Inodes in all Media Extents Combined	Total number of inodes in all storage volumes allocated for a Snapshot Container.
Number of Inode Allocated	Number of inodes allocated for snapshot operation.
Number of Data Area Section in all Media Extents Combined	Number of Data Area Sections in all storage volumes allocated for a Snapshot Container.
Number of Data Area Section Allocated	Number of Data Area Sections consumed for the current snapshot operation.
Snapshot Set	
LD/LV, Partition	The unique ID of the source volume this Snapshot Set is referring to.
Activated	A snapshot image has been created in the Snapshot Set.
Mount Status	Array status (the status of the RAID array that this Snapshot Set is referring to).
Data Block Size	Data blocks consumed by the Snapshot Images in this Snapshot Set.
Current Active Snapshot Image ID	The unique ID(s) of the currently activated Snapshot Image(s).
Snapshot Image	
Activation Sequence Number	When a snapshot image is activated, it appears as a frozen image that can be mapped to a host LUN. The act of taking a snapshot image actually include creating and activating a snapshot image.

	The sequence number indicates the image's positions among a series of snapshot images.
Activated Actual Time	Indicates the time when the image was taken.
Last Modification Time	The last time when the source volume receives updates and differentials were added to a snapshot image.
Activation Schedule Time	Applies to Snapshot Scheduler. The time refers to when the scheduler creates and activates a snapshot image.
Total Number of Data Block Entries	The total number of data block entries reserved for a snapshot image.
Valid Data Block Entries already Filled	Numbers of data block entries consumed by storing data differentials.
Total Data Block Entries already Filled	Numbers of data block entries consumed by data differentials including valid and bad blocks.

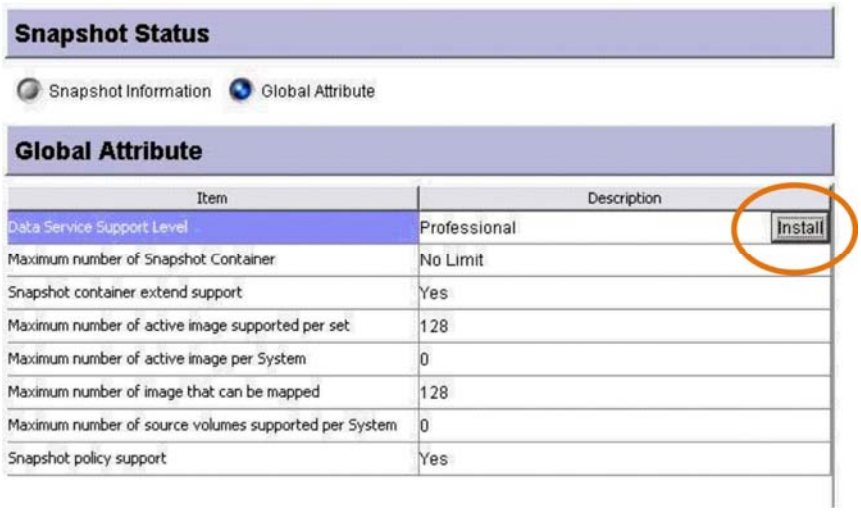
Media Extent List



Snapshot Container ID	A single click on one of the Snapshot Containers displays the related information. Snapshot Container ID is a unique identifier randomly generated by firmware.
Status	The status of the Snapshot Container. Online means a valid SC configuration. Offline refers to degraded states such as a logical drive failure.
Data Area Section Size	The size of smallest allocation unit in snapshot data differentials. Similar to data blocks in ordinary storage media.
Mount Status	Array status (Status of the Source Volume that this Snapshot Container is referring to).
Current/Max. Media Extent	The number of RAID volume (LD, LV, or partitions) currently contained within this Snapshot Container and the max. number of volumes allowed.

Inode Table Entry Size	Inode refers to the infrastructure table used to organize data differentials, differential locations, and relational information
Total Number of Inodes in all Media Extents Combined	Total number of inodes in all contained storage volumes allocated for a Snapshot Container.
Number of Inode Allocated	Number of inodes allocated for snapshot operation.
Number of Data Area Section in all Media Extents Combined	Number of Data Area Sections in all storage volumes allocated for a Snapshot Container.
Number of Data Area Section Allocated	Number of Data Area Sections consumed for the current snapshot operation.

Global Attribute

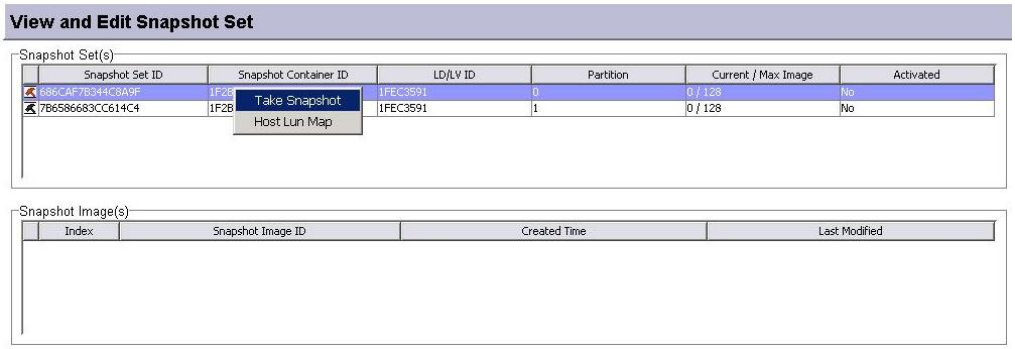


The **Global Attribute** window generally reflects the capabilities and limitations of your SANWatch version, either **Express** or the **Professional** version.

The **Install** button on the upper right initiates the License Key application window when you need to upgrade SANWatch Data Service functionality.

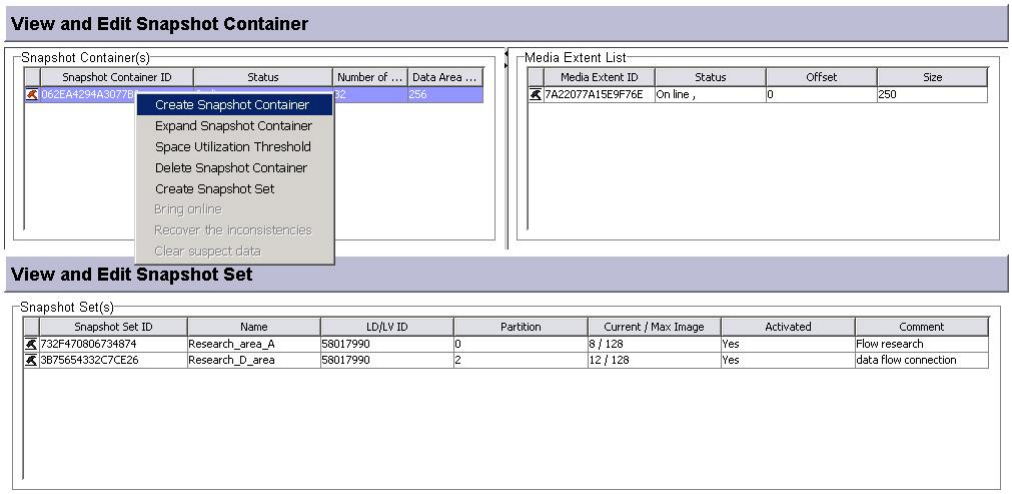
Data Service Support Level	Shows whether your SANWatch supports the Express or Professional level of Snapshot functionalities. The Professional level supports automated snapshot prune and the Snapshot Scheduler functionality.
Maximum number of snapshot container	The maximum number of Snapshot Containers.
Snapshot container extend support	Shows whether your SANWatch support Snapshot Container expansion.
Maximum number of active image supported per set	The maximum number of active images per Snapshot Set.
Maximum number of active image per System	The maximum number of active images per RAID system.
Maximum number of image that can be mapped	The maximum number of images that can be mapped to host LUNs for data retrieval.
Maximum number of source volumes supported per system	The maximum number of source volumes per system. This number is determined by the number of disk drives, and the maximum number or RAID configuration units.
Snapshot policy support	Snapshot prune and purge support.

Maintain Snapshot: contains functions that allow you to manually take snapshots or associate a snapshot image with a host ID/LUN.



Configure Snapshot: provides access to snapshot-related commands including:

- Create Snapshot Container
- Expand Snapshot Container
- Delete Snapshot Container
- Create Snapshot Set
- Fault recovery commands



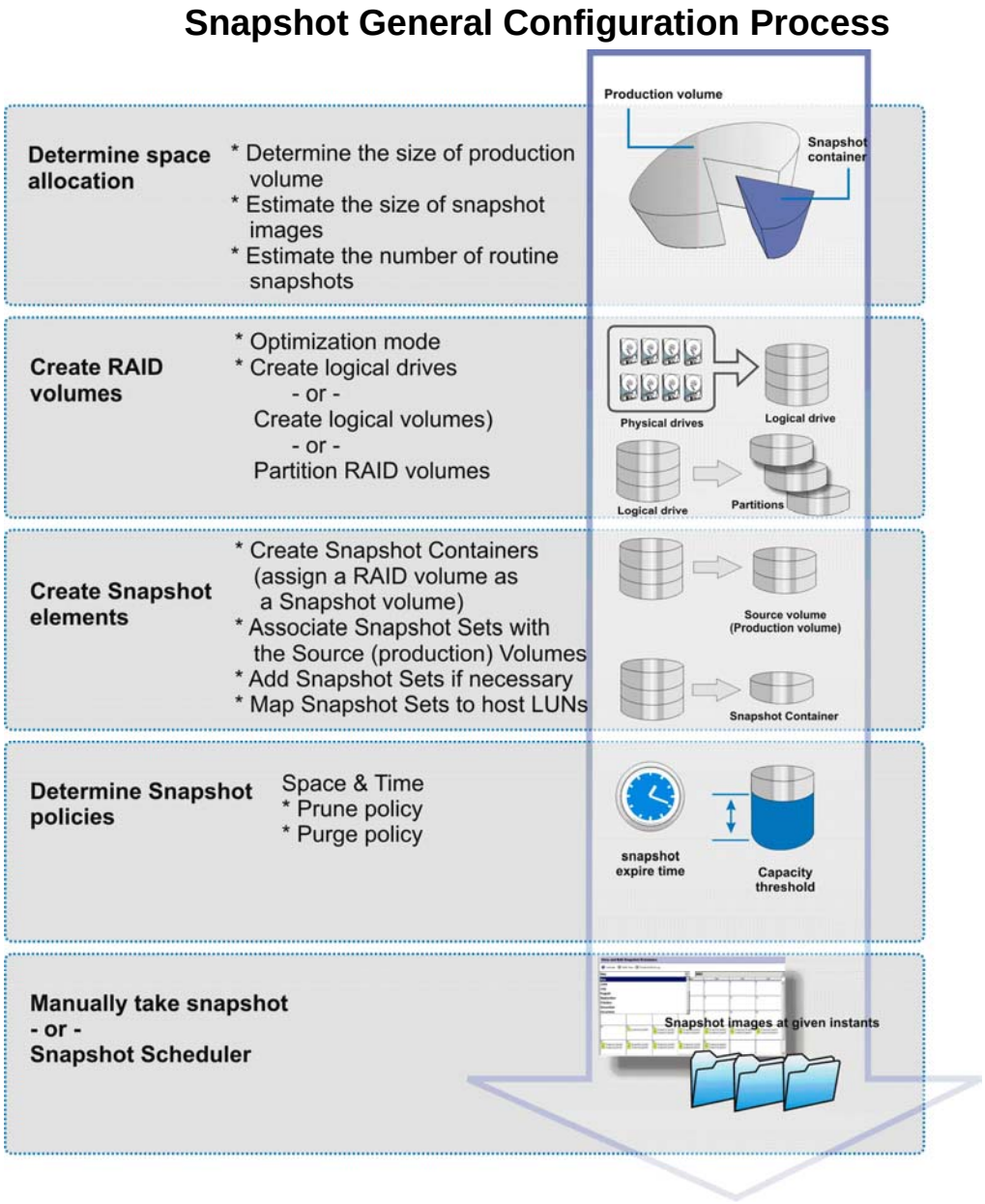
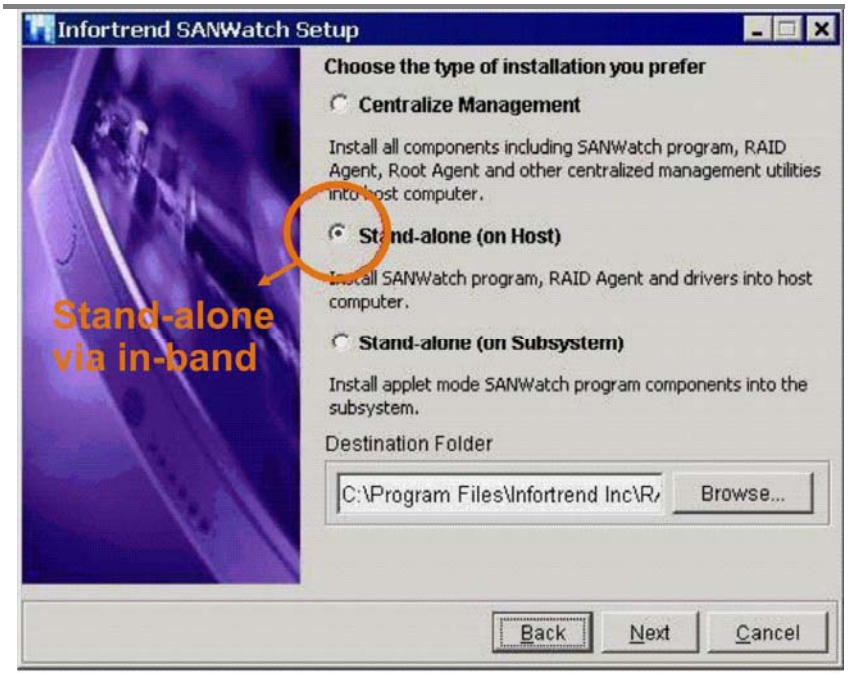


Figure 15-5: Snapshot General Configuration Process

NOTE:

The automated **purge, prune** policies, and the automated **Snapshot scheduler** are currently applicable with flush agent support. They are available in applications where SANWatch is installed on an application server that is directly attached to a RAID storage, and where the SANWatch-to-storage communication is made through the in-band protocols.

The in-band support is available by installing SANWatch using the **Custom** -> **Stand-alone (on Host)** mode.


Infortrend SANWatch Setup
Stand-alone via in-band
Choose the type of installation you prefer
Centralize Management
Install all components including SANWatch program, RAID Agent, Root Agent and other centralized management utilities into host computer.
Stand-alone (on Host)
Install SANWatch program, RAID Agent and drivers into host computer.
Stand-alone (on Subsystem)
Install applet mode SANWatch program components into the subsystem.
Destination Folder
C:\Program Files\Infortrend Inc\R
Browse...
Back
Next
Cancel

To access a directly-attached RAID storage via in-band protocols, enter the server's IP in the **Connection** wizard. The RAID agents running on the application server will manage the management access.

Configuration Steps:

Step 1. Determine Space Allocation:

Although the point-in-time snapshot takes comparatively small storage space, it is imperative that you create a reasonable amount of individual storage volumes in case your snapshots take up too much storage space and use it up too quickly.

Logical partitions are more convenient in planning space allocation. There are two reasons for this:

1. Reconfiguring a RAID configuration (e.g., reconfiguring a logical drive) requires moving data, deleting, and re-creating an existing logical drive.
2. Although an Infortrend RAID enclosure can contain up to 16 or 24 disk drives, there is actually a limited number of logical drives especially if you are using the high redundancy RAID level such as RAID6. Two parity disks are required for each RAID6 array and the usable disk space will thus be compromised.

Using RAID partitioning is not a must; however, you are given more elbow room with planning your storage space:

1. You may create one or two source volumes (two logical drives) which serve as the production volumes (those that service host I/Os).
2. You may use another logical drive, partition it, and use one of the partitions to contain the snapshot images of the two source volumes.
3. You may reserve some of the RAID partitions for future expansion. Snapshot Containers can be expanded using the unused partitions, just in case the amount of updates exceeds your original expectation.

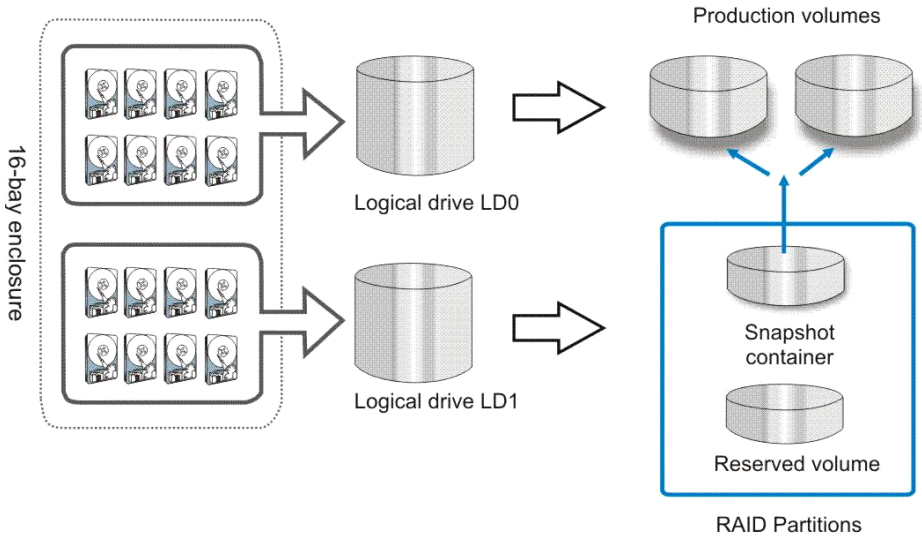


Figure 15-6: Array Space Allocation in Snapshot Application

Depending on how frequently snapshots are taken and how frequently the data in source volumes are changed, the proportion between source volumes and snapshot volumes can vary.

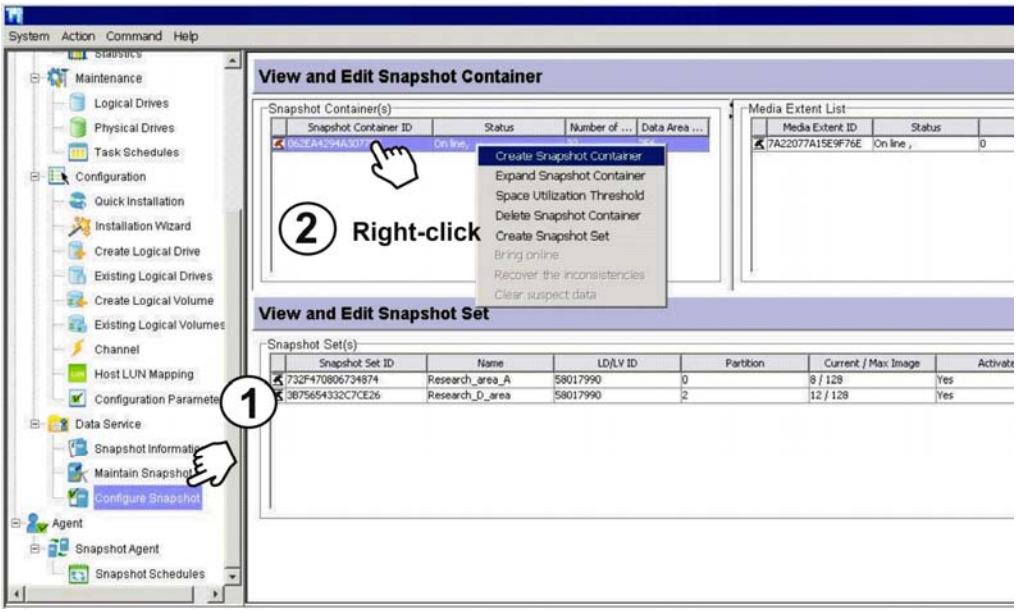
You may use the above diagram as an example and draw your own configuration scheme, listing physical drives, logical drives/volumes/partitions, and then the source volumes and Snapshot Containers, etc.

Step 2. Create RAID Volumes:

Follow normal RAID configuration procedures to optimize array performance preferences, create logical drives, logical volumes, logical partitions, and host LUN mapping. You may also reserve some of the disk drives as hot-spares.

Step 3. Create Snapshot Elements

Step 3-1. Create a Snapshot Container:



Step 3-1-1. Click on the **Configure Snapshot** icon in the navigation tree menu on the left-side of the GUI screen.

Step 3-1-2. Right-click in the **Snapshot Container** field to display the "**Create Snapshot Container**" command.

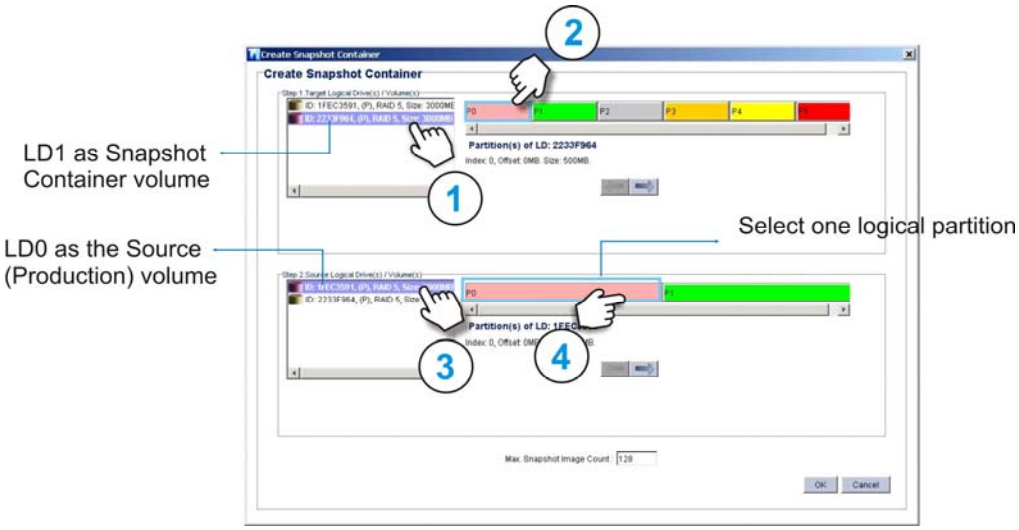
Step 3-1-3. Click on the command. A selection window appears showing two subordinate steps.

Step 1 allows you to select a **RAID volume** (or a partition of it) as the Snapshot Container.

Step 2 allows you to select a **Source volume** for the first Snapshot Set in this Snapshot Container to refer to.

Note that the **FIRST Snapshot Set** under this container will be automatically created and will refer to this source volume.

You may select a different RAID partition (if configured) by a single mouse-click on one of the color bars. Each RAID partition within a RAID volume is displayed in a different color.



Step 3-1-4. Click **OK** to complete the process.

NOTE:

It is a good practice to keep a configuration diagram showing information such as the number of logical drives, logical partitions, their capacities, and their roles. In a complex configuration, you can easily get lost in a jungle of logical configurations.

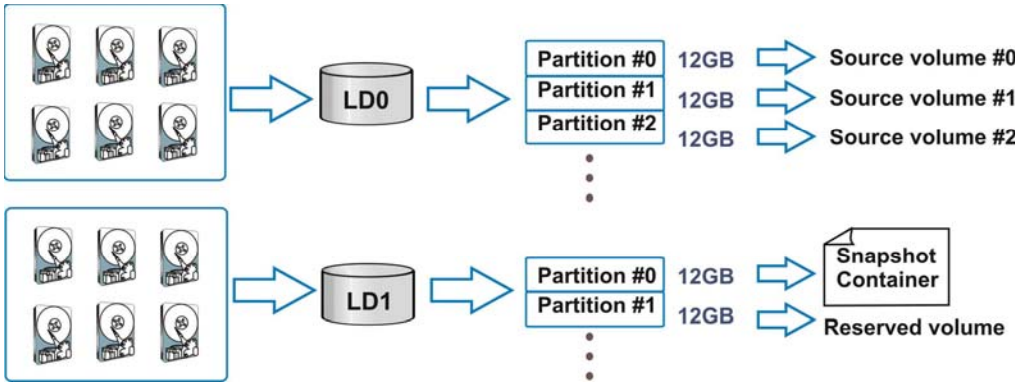


Figure 15-7: Exemplary RAID and Snapshot Configuration Drawing

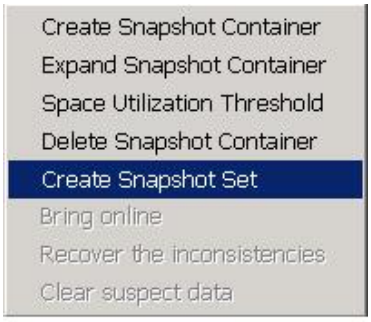
Step 3-2 Create an Additional Snapshot Set

NOTE:

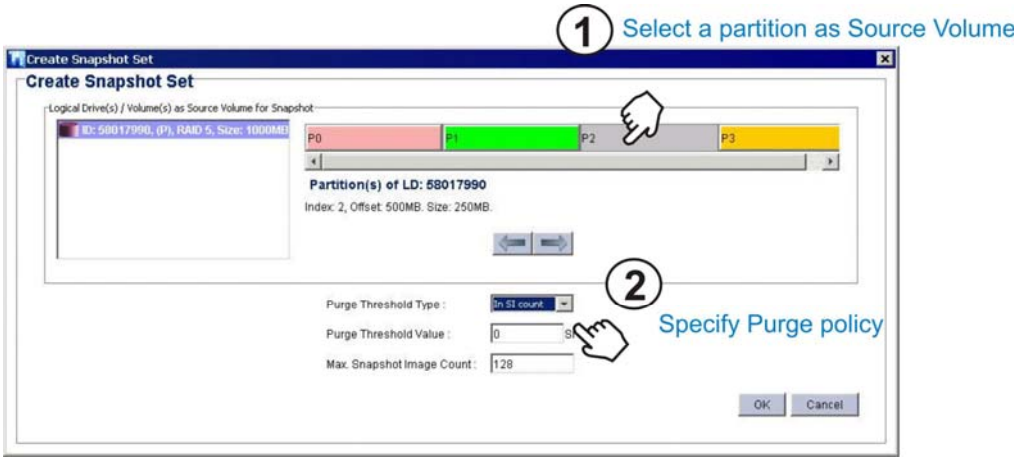
A **Snapshot Set** is automatically created whenever a Snapshot Container is created. Multiple Snapshot Sets can be manually added to a Snapshot Container in order to refer to other source volumes.

Step 3-2-1. Click on the **Configure Snapshot** icon in the navigation tree, and then single click to select an existing Snapshot Container.

Step 3-2-2. Right-click on an existing Snapshot Container and select "**Create Snapshot Set**" from the dropdown list.



Step 3-2-3. A selection window appears showing configured RAID volumes. Click on a RAID volume in the "**Logical Drive(s)/Volume(s)**" column, and click on a color bar to select a RAID partition (if configured).



Step 3-2-4. Select **Purge Threshold** parameters from the dropdown lists in the lower half of the screen.

Purge Threshold Type:

In Time(secs) – Specify the purge threshold type as how long the Snapshot images will be kept.

In SI count – Specify the purge threshold type as how many Snapshot images will be kept for the Snapshot Set.

Purge Threshold Value: Enter a threshold value here.

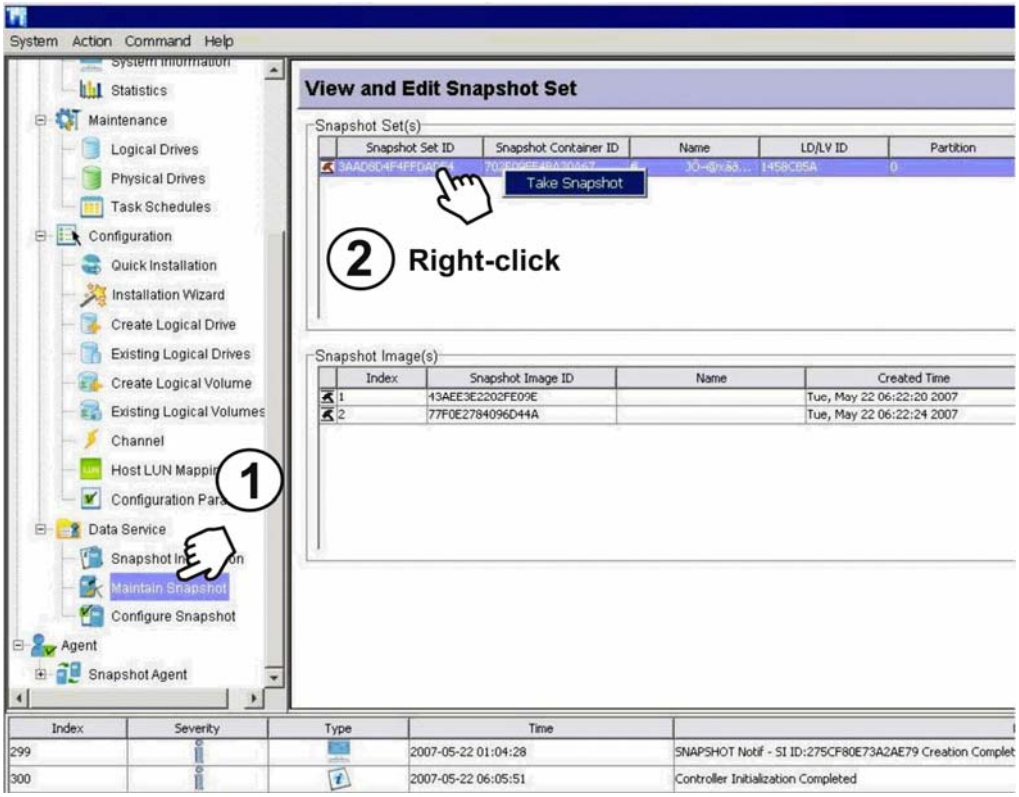
Max. Snapshot image Count: The default for the maximum number of Snapshot images is shown.

Step 3-2-5. Click **OK** to complete the process.

Step 3-3. Taking Snapshots: Manually Create Snapshot Images

CAUTION!

Before manually taking a snapshot, free host I/Os and flush OS and application caches to avoid data inconsistency.



Step 3-3-1. Select "**Maintain Snapshot**" from the left-side navigation tree. Select an existing Snapshot Set and then right-click on it to display the "**Take Snapshot**" command.

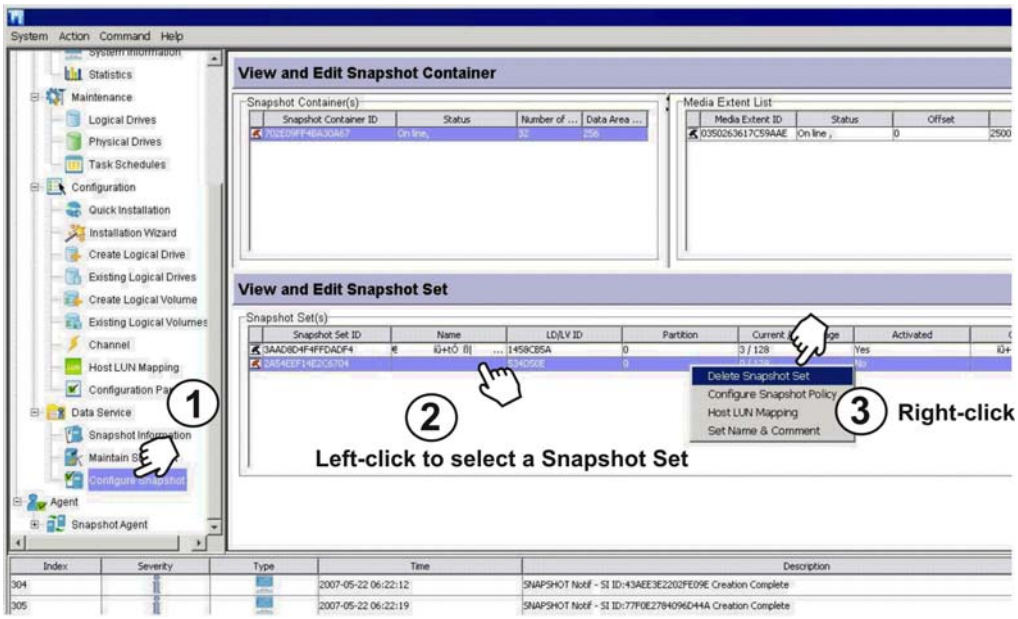
Step 3-3-2. Click on the "**Take Snapshot**" command.

Step 3-3-3. The snapshot is taken almost immediately and the snapshot images appear in the **Snapshot Image** field on the lower half of the screen.

Step 3-4. Snapshot Set Mapping

IMPORTANT!

If a source volume has already been mapped to a host ID/LUN, it is recommended you unmap the source volume and then create snapshot configuration for this volume. This may require that you stop the currently running applications.



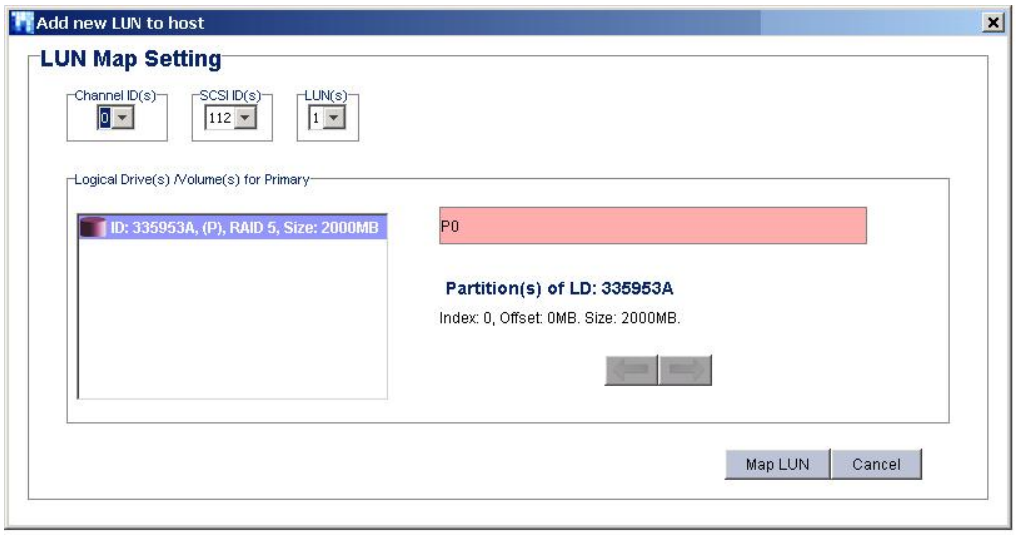
NOTE:

Mapping a Snapshot Set is actually mapping the Source Volume it is referring to.

Step 3-4-1. Select "**Configure Snapshot**" from the left-side navigation tree.

Step 3-4-2. Left-click on an existing **Snapshot Set** under the "**View and Edit Snapshot**" field. A selected Snapshot Set will be highlighted. Right-click on it to display a command menu.

Step 3-4-3. Select **Host LUN Mapping**. A Host LUN mapping window displays.



Step 3-4-4. Select **Host Channel**, **Channel ID**, and/or **LUN** numbers from the respective dropdown lists on the upper left of the screen. Click on the **Map LUN** button to complete the process.

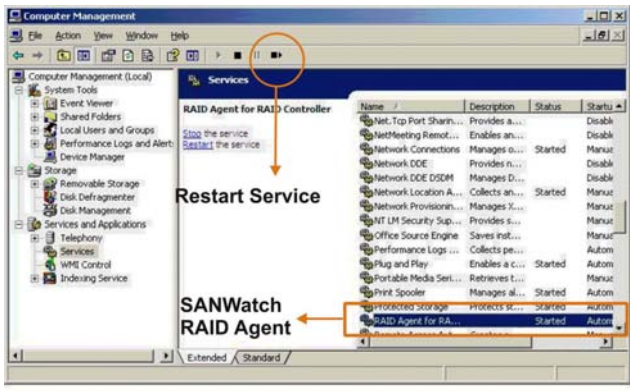
NOTE:

If the source volume has already been mapped to a host ID/LUN, you may not be able to map the associated Snapshot Set.

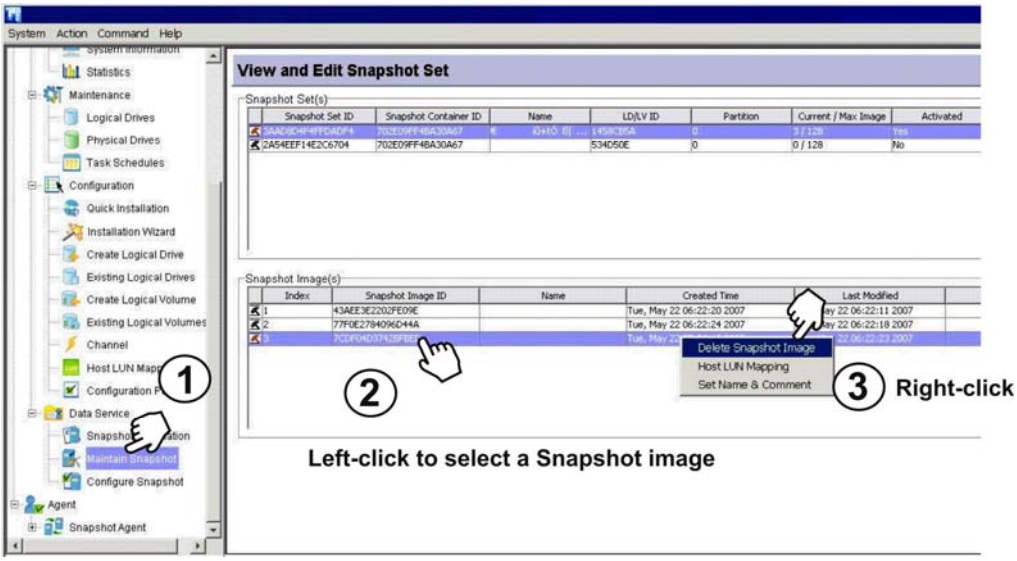
If the source volume has not been mapped, it is recommended you perform host LUN mapping from here. Mapping a Snapshot Set is actually equal to mapping the source volume it is referring to.

TIPS:

Under some circumstances, unmapping a RAID volume may temporarily disconnect a SANWatch console. You may manually restart SANWatch RAID agent in, for example, Windows Computer Management -> Services in order to restore the console.



Step 3-5. Data Retrieval: Snapshot Image Mapping



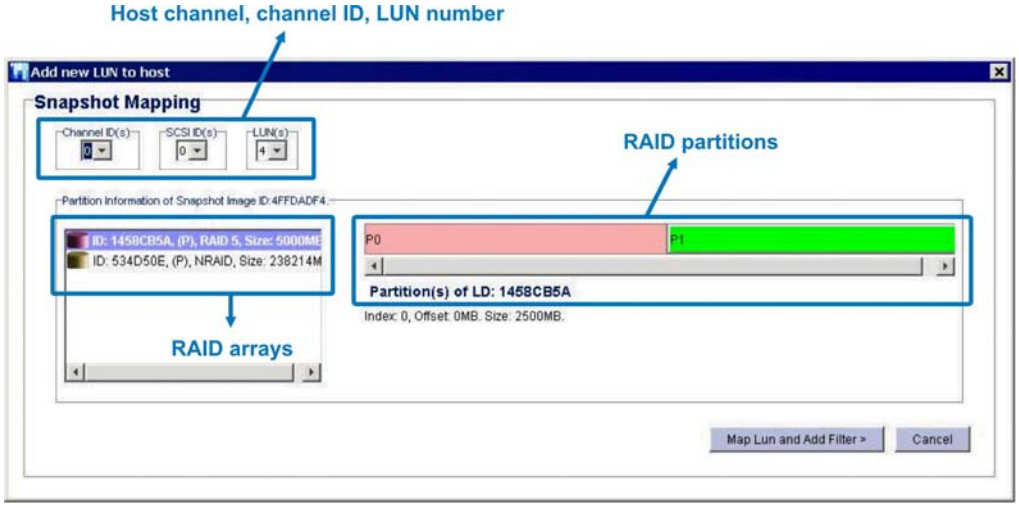
Step 3-5-1. Select **Maintain Snapshot** on the navigation tree by a single mouse click.

Step 3-5-2. Left-click on an existing Snapshot Set on the upper half of the screen. The subordinate snapshot images will display in the lower half of the configuration screen.

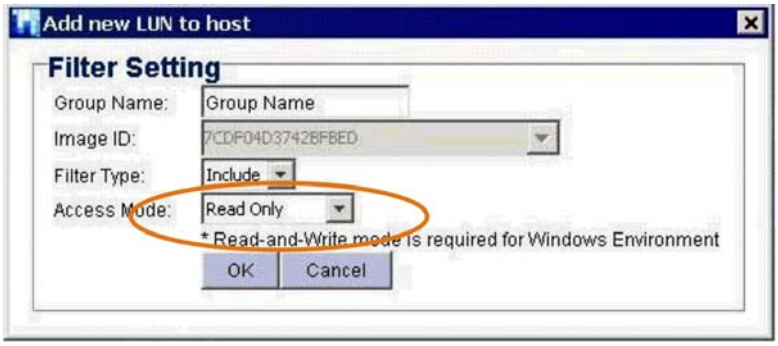
Step 3-5-3. Left-click to select an image, and right-click on an existing Snapshot Image to display the **Host LUN Mapping** command.

Step 3-5-4. Select **Host Channel**, **Channel ID**, and/or **LUN** numbers from the associated dropdown lists on the pop-up mapping window. The associated RAID arrays and RAID partitions are for display only. They refer to the original source volume for which the snapshot was taken.

Step 3-5-5. Click on the **Map LUN and Add Filter** button to complete the process.



Step 3-5-6. A **Filter Setting** window will prompt. Select "**Read-and-Write**" from the **Access Mode** for a Windows platform. The Windows OSes file system needs to write registration metadata onto a storage volume, and hence the access mode needs to be changed here.



NOTE:

Note that SANWatch only allows Windows file system to distribute metadata. In order to avoid destroying the original data differentials, the snapshot image volumes will still be "Read-Only" volumes.

Mapping a Snapshot Image to a host ID/LUN avails the image as a read-only volume. A mapped image is its source volume at the time when the snapshot image was taken. Mapping a Snapshot Image provides you access to the original data at a given instant.

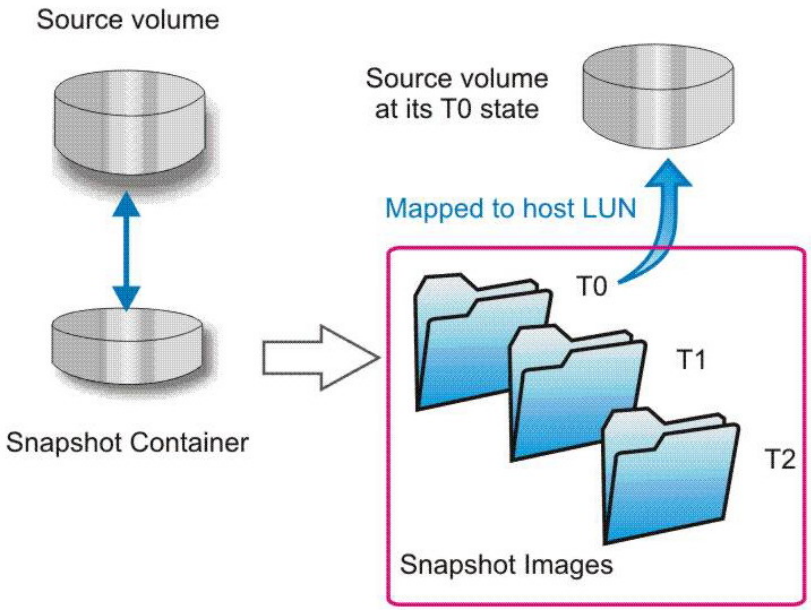
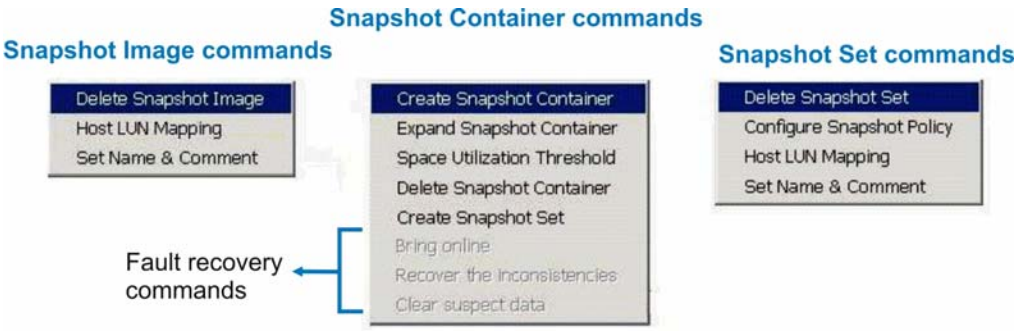


Figure 15-8: Snapshot Image Mapped to Host ID/LUN (Data Retrieval)

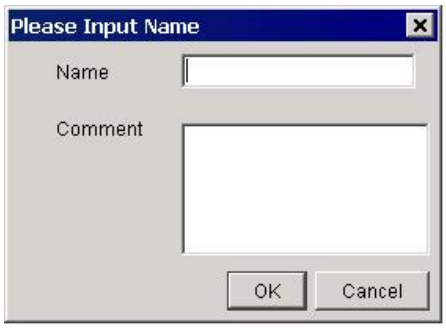
NOTE:

Snapshot Recovery, using a Snapshot Image to restore a Source Volume to the state at a given instant, is not yet available in this release.

Other Commands:



1. **Delete Snapshot Set/Snapshot Container/Snapshot Image**: Allows you to manually remove a snapshot element.
2. **Set Name & Comment**: This command brings forth an input window with two text boxes that allow you to put a name tag and description for a specific Snapshot Image or Snapshot Set.



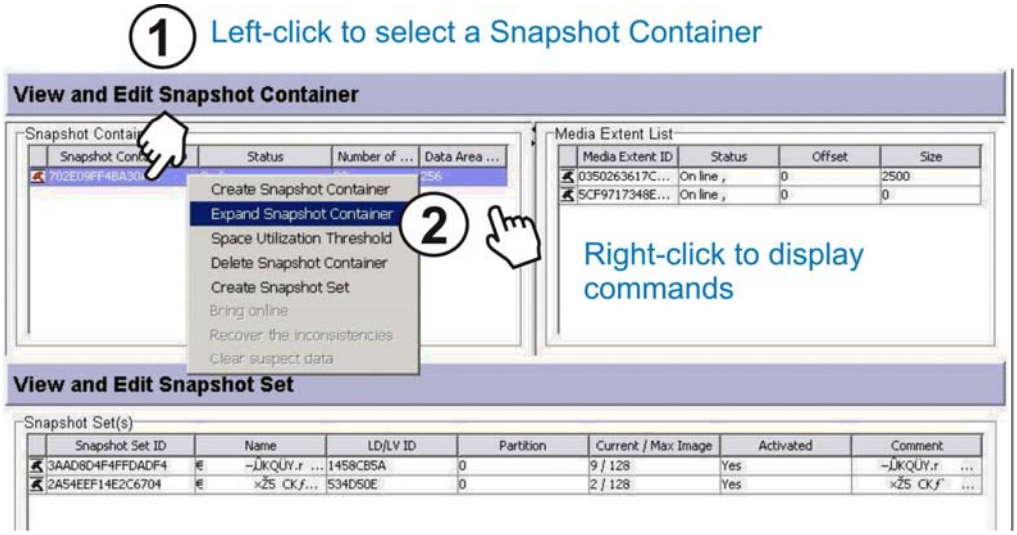
3. **Expand Snapshot Container**: This command allows you to expand an existing Snapshot Container by joining in another RAID partition/volume.

   You can join another RAID partition with the Snapshot Container volume currently in use. Free space can also be acquired by expanding logical drives.

   NOTE that once you join a RAID partition into an existing Snapshot Container, you cannot separate them after the expansion.

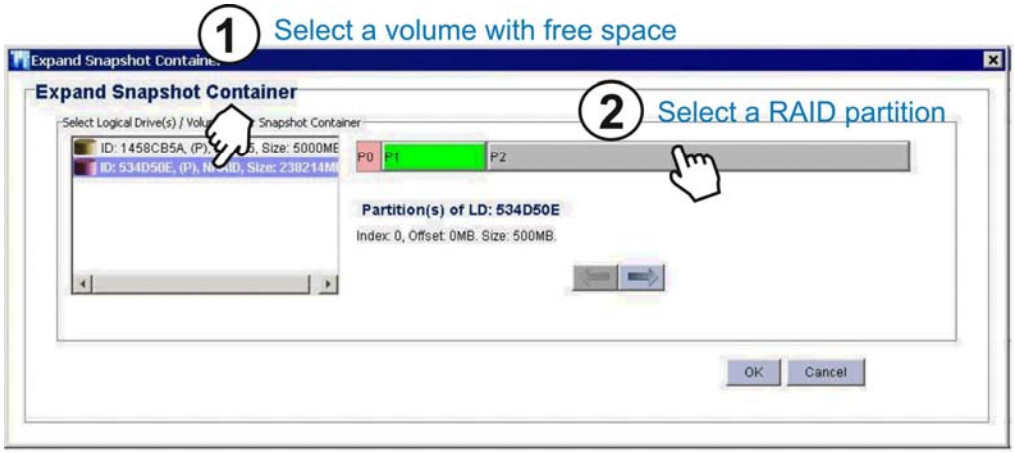
To expand a Snapshot Container,

Step 1. Left-click to select a Snapshot Container.



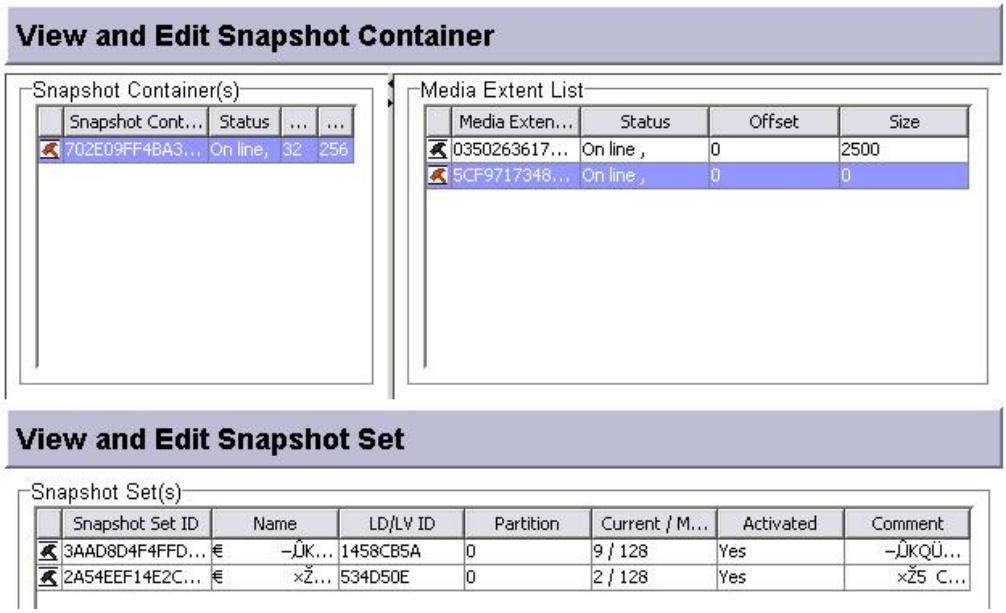
Step 2. Right-click to display the configuration commands. Left-click on the **Expand Snapshot Container** command.

Step 3. A volume selection window will prompt. Use a single click to select a RAID volume with free space, and then select an unused partition.



Step 4. Click the OK button to complete the process.

As shown below, the added partition will be listed in the Media Extent List.



4. **Fault Recovery Commands**: These commands apply only when system faults occur. For some reasons, the snapshot cannot write to disk drives, or fail to read data from Snapshot Containers or Snapshot Sets. Read/write errors could result from drive media errors or the inconsistencies between cached data and data on drive media. The Fault Recovery commands can be used to recover the inconsistencies after media faults or logical drive errors are corrected.

5. **Configure Snapshot Policy + Space Utilization Threshold**: These commands belong to the automated Snapshot management. See the following section for details.

15.3 Snapshot Purge Policy (Space Management)

The Snapshot Purge policy help contain the storage capacity taken up by the snapshot operation. When properly configured, the purge policy ensures there is sufficient space in case you need to retrieve snapshot data from snapshot images.

15.3.1 What Are the Differences between Purge and Prune Policies?

A default 70% upper threshold comes with each Snapshot Container.

Purge Policy: The Purge action is triggered by a capacity threshold value on a specific Snapshot Container. Once the threshold is exceeded, SANWatch will start erasing previous images in order to release storage space. The purge action will continue until there remains a reserve of the minimum number of snapshot images. The reserve can be configured as the minimum number of snapshot images or by the life span of individual snapshot images.

For example, if snapshots' life span is set to "one week" and a snapshot is taken every day, a Purge action desperately freeing capacity will eventually stop by the reserve consisting of seven images.

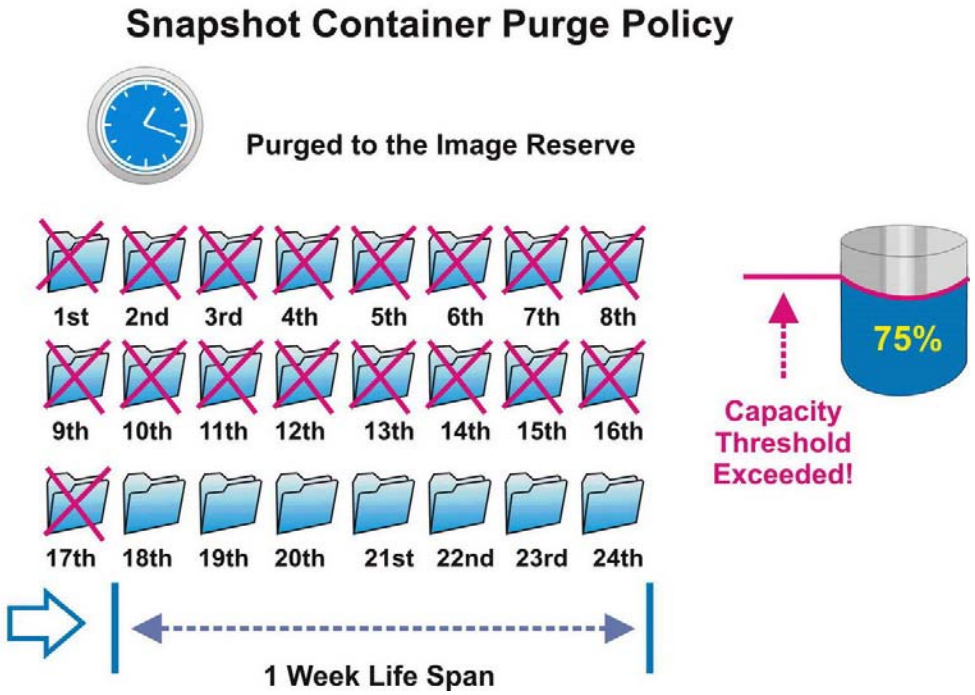


Figure 15-9: Snapshot Purge Policy (with Life Span Setting)

Prune Policy: The Prune policy is bundled with the automated **Snapshot Scheduler** utility (see the following section) as the "**upper**" threshold on how many snapshot images to be taken and maintained by a Snapshot schedule.

Shown below is an example with a "one week" life span threshold. If one snapshot is taken each day, the first image will be erased on the eighth day.

The scheduler prune policy helps contain the number of snapshot images taken by each snapshot schedule.

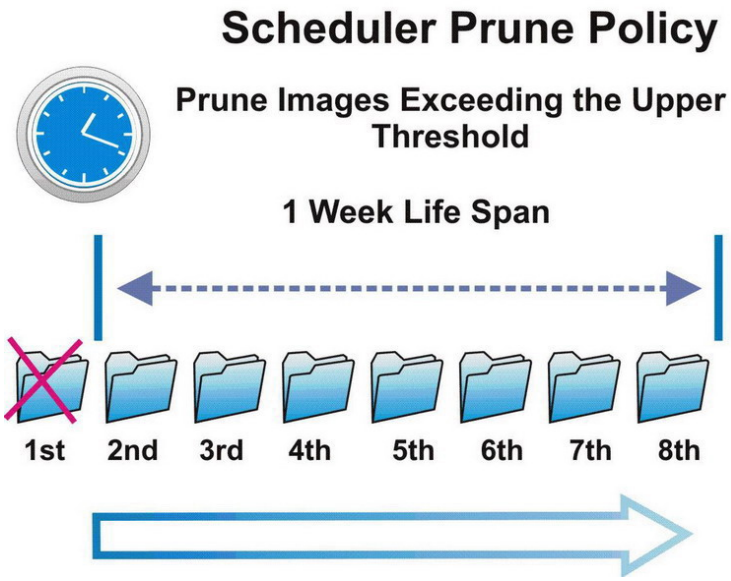


Figure 15-10: Snapshot Prune Policy (with Life Span Setting)

TIPS:

You can check capacity usage in the **Snapshot Information** window by clicking on a Snapshot Container/Set, and then scroll down to see a **percentage graph**.

15.3.2 Purge Policy Configuration

The Purge Rule policy can be configured on an existing Snapshot Container or a Snapshot Set. For example, if there are two Snapshot Sets under a Snapshot Container, you can set a 50% purge policy on one of them in order to control the maximum space used by each Snapshot Set.

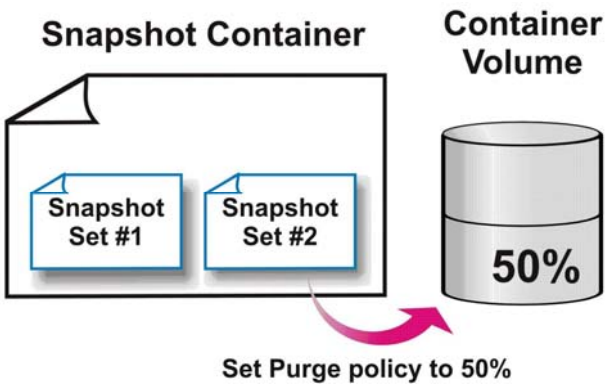
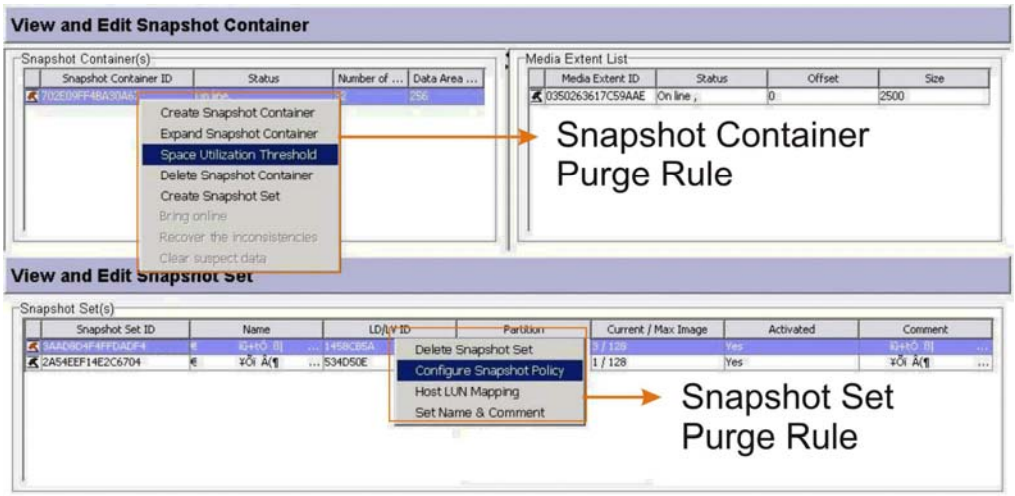


Figure 15-11: Purge Policy on One of the Snapshot Sets



Purge Policy with Snapshot Container:

Step 1. Under the **View and Edit Snapshot Container** screen, click to select a Snapshot Container.

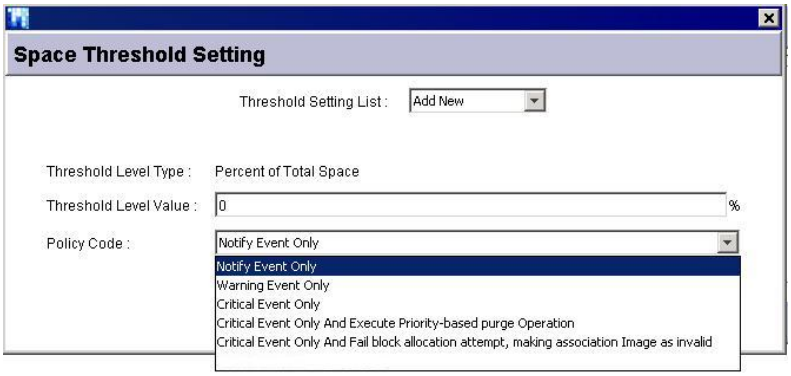
Step 2. Right-click to display the related commands, and left-click on **Space Utilization Threshold**.

Step 3. Your will be prompted by a **Space Threshold** window. Use the dropdown lists to specify a capacity threshold for a specific container.

Threshold Level Value: Enter a percentage number in the text field. When a percentage threshold is

violated, the automated purge control will be initiated.

Policy Code: Select an option from the pull-down list.



The purge control options include:

Notify Event only: A notification level event message will be delivered to notify system administrator.

Warning Event only: A warning level event message will be delivered to notify system administrator.

Critical Event only: A critical level event message will be delivered to notify system administrator.

Critical Event only and Execute Priority-based purge Operation:

1. A critical level event message will be delivered to notify system administrator.
2. System starts removing the highest purge priority Snapshot images in order to release storage space.

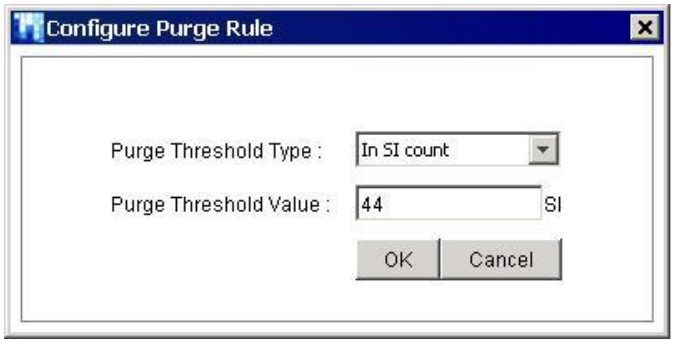
Critical Event only and Fail block allocation attempt, making association Image as Invalid:

1. A critical level event message will be delivered to notify system administrator.
2. System stops the snapshooting operation that is currently taking place.

Purge Policy with Snapshot Set:

Step 1. Under the **View and Edit Snapshot Set** screen, click to select a Snapshot Set.

Step 2. Right-click to display the related commands, and left-click on **Configure Snapshot Policy**.



Step 3. A Purge Rule window will appear. Configure you preferences through the dropdown lists and the text field.

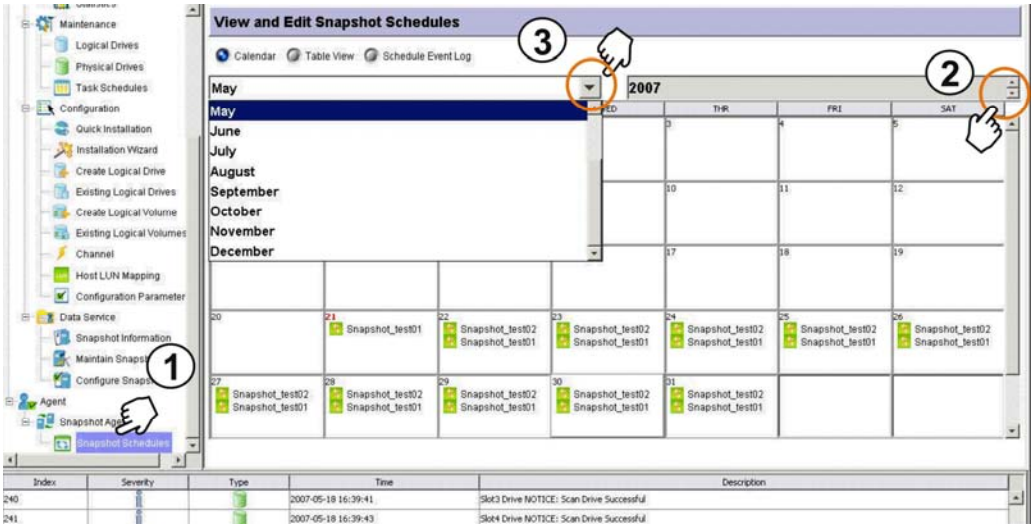
The following two parameters determine the minimum number of snapshot images to be preserved when system purges old snapshots.

Purge Threshold Type: You may select a threshold type here as the life span of snapshot images or as the number of snapshot images. Selecting a different type changes the reckoning unit of the following threshold value.

Purge Threshold Value: Enter either the life span in seconds or the number of snapshot images to be preserved in the text field.

15.4 Snapshot Scheduler & Prune Policy Configuration

The **Prune Policy** options are found during the Snapshot Scheduler configuration procedures.

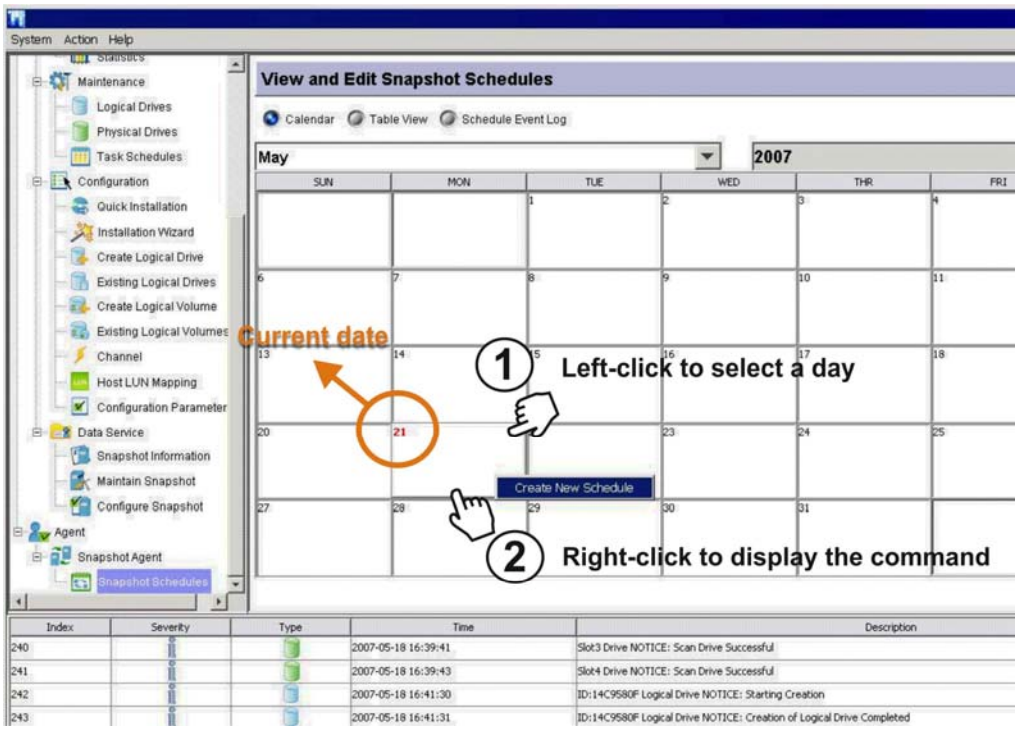


Step 1. Open the **Snapshot Schedules** view by a single click on its icon on the navigation tree.

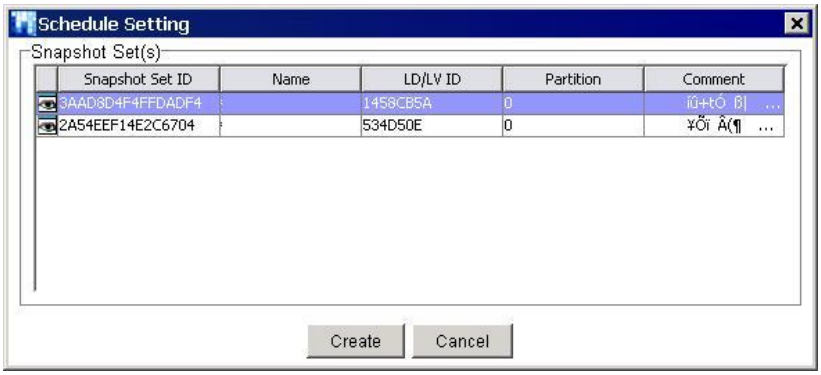
Step 2. Select a calendar by selecting the year and month dropdown lists. As long as your system date and time has been properly configured, there should be no troubles with the default calendar.

Step 3. Select a day by a single mouse click. A selected date will look a little afloat than other entries on the calendar.

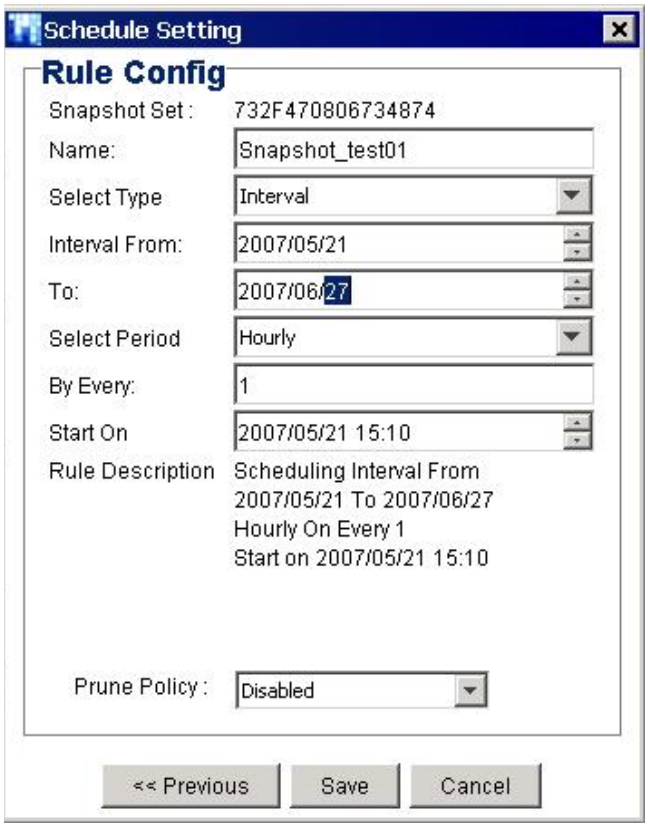
Step 4. Right-click on a day to activate the **Create New Schedule** command.



Step 5. A **Snapshot Set** selector window appears. Select a Snapshot Set by a single mouse click, and click on the **Create** button to proceed.



Step 6. Another **Schedule Setting** window will prompt, providing you various options with starting an automated snapshot schedule.



Below are details about setting each configurable scheduler option:

Name: Provide a name for the schedule. Letters and numeric characters are preferred.

Select Type: **Once** – A Snapshot will be taken just once. When Once is selected, the below options will be grayed out.

Interval – Snapshots will be taken at specified intervals between a begin date and an end date.

Repeatedly – Snapshots will be taken at specified intervals without the limitation of a begin date and an end date.

Interval From: The begin date of the **Interval** type of snapshot schedule.

The begin and end date can be changed by double-clicking a number (as highlighted in the screen above), and then click on the up or down buttons to increase or decrease the number.

To: The end date of the **Interval** type of snapshot schedule.

Select Period: Specify the interval between two snapshots. Options are **Hourly**, **Daily**, **Weekly**, and **Monthly**.

By Every: The unit of reckoning you selected previously in the **Select Period** field will be multiplied by the number you enter in this field, e.g., 2 x Hourly = every two hours.

Start On: Use the previous stipulated method to change the start time of the schedule.

Prune Policy: The Prune Policy field allows you to control the number of snapshot images by setting the following:

Snapshot Image Count: The maximum number of snapshot images to be taken by this schedule. When the maximum number of snapshot images is exceeded, the oldest snapshot will be erased.

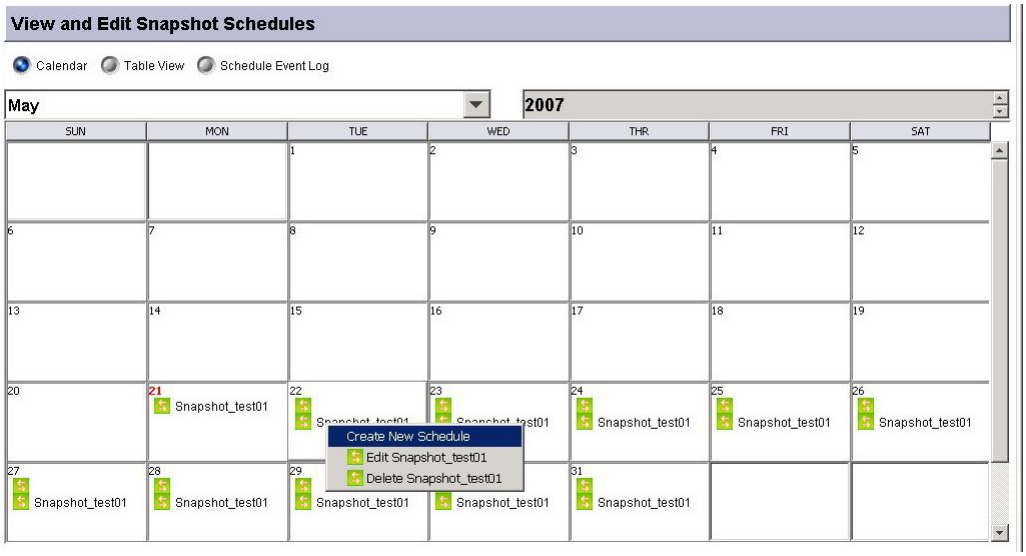
Expire Time: When selected, enter the number of days as the snapshot life span. Any images older than that will be automatically erased.

Rule Description: The Rule Description briefly summarizes your current configuration for the schedule.

Click on the **Save** button to confirm your configuration. Click on the **Cancel** button to abandon your current configuration.

Click on the **<< Previous** button to select a different Snapshot Set.

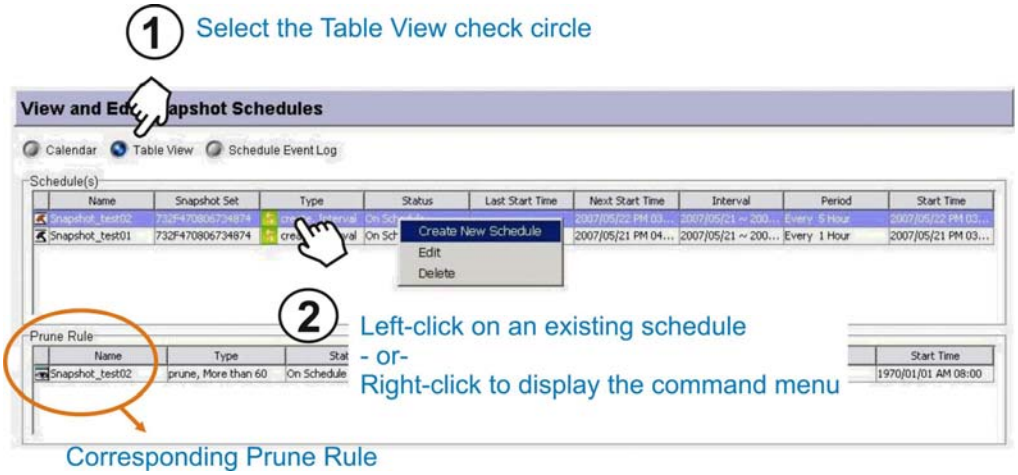
Once done, the Scheduler calendar will look like the screen below:



Planned schedules will be listed on the calendar. You can select a day, and then right-click to display the **Create New Schedule**, **Edit**, or **Delete** schedule commands.

Table View and Scheduler Events

To access the Table View, click on the Table View check circle.

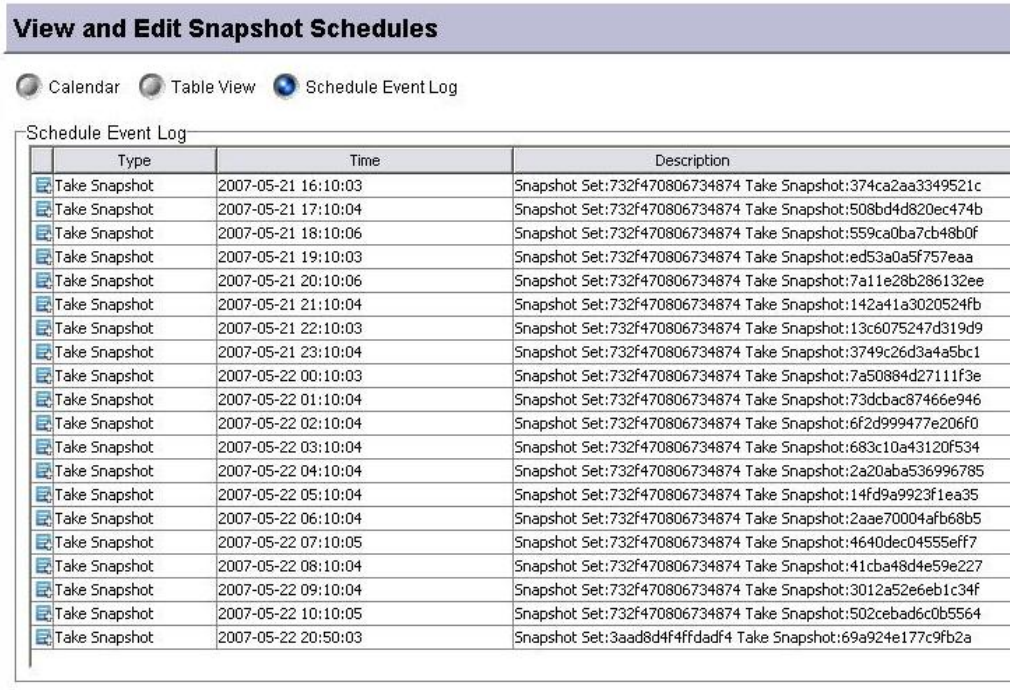


You may select an existing schedule by a mouse click, or right-click on the **Schedule(s)** list to display the Scheduler commands.

Use the same method described previously in the **Calendar View** configuration procedure to create, edit, or delete a schedule.

The **Prune Rule** column at the lower screen provides information about the Prune policy settings bundled with each snapshot schedule.

Schedule Event Log



Type	Time	Description
Take Snapshot	2007-05-21 16:10:03	Snapshot Set:732f470806734874 Take Snapshot:374ca2aa3349521c
Take Snapshot	2007-05-21 17:10:04	Snapshot Set:732f470806734874 Take Snapshot:508bd4d820ec474b
Take Snapshot	2007-05-21 18:10:06	Snapshot Set:732f470806734874 Take Snapshot:559ca0ba7cb48b0f
Take Snapshot	2007-05-21 19:10:03	Snapshot Set:732f470806734874 Take Snapshot:ed53a0a5f757eaa
Take Snapshot	2007-05-21 20:10:06	Snapshot Set:732f470806734874 Take Snapshot:7a11e28b286132ee
Take Snapshot	2007-05-21 21:10:04	Snapshot Set:732f470806734874 Take Snapshot:142a41a3020524fb
Take Snapshot	2007-05-21 22:10:03	Snapshot Set:732f470806734874 Take Snapshot:13c6075247d319d9
Take Snapshot	2007-05-21 23:10:04	Snapshot Set:732f470806734874 Take Snapshot:3749c26d3a4a5bc1
Take Snapshot	2007-05-22 00:10:03	Snapshot Set:732f470806734874 Take Snapshot:7a50884d27111f3e
Take Snapshot	2007-05-22 01:10:04	Snapshot Set:732f470806734874 Take Snapshot:73dcbac87466e946
Take Snapshot	2007-05-22 02:10:04	Snapshot Set:732f470806734874 Take Snapshot:6f2d999477e206f0
Take Snapshot	2007-05-22 03:10:04	Snapshot Set:732f470806734874 Take Snapshot:683c10a43120f534
Take Snapshot	2007-05-22 04:10:04	Snapshot Set:732f470806734874 Take Snapshot:2a20aba536996785
Take Snapshot	2007-05-22 05:10:04	Snapshot Set:732f470806734874 Take Snapshot:14fd9a9923f1ea35
Take Snapshot	2007-05-22 06:10:04	Snapshot Set:732f470806734874 Take Snapshot:2aae70004afb68b5
Take Snapshot	2007-05-22 07:10:05	Snapshot Set:732f470806734874 Take Snapshot:4640dec04555eff7
Take Snapshot	2007-05-22 08:10:04	Snapshot Set:732f470806734874 Take Snapshot:41cba48d4e59e227
Take Snapshot	2007-05-22 09:10:04	Snapshot Set:732f470806734874 Take Snapshot:3012a52e6eb1c34f
Take Snapshot	2007-05-22 10:10:05	Snapshot Set:732f470806734874 Take Snapshot:502cebad6c0b5564
Take Snapshot	2007-05-22 20:50:03	Snapshot Set:3aad8d4f4ffdadf4 Take Snapshot:69a924e177c9fb2a

The **Schedule Event Log** is opened by clicking its check circle. The event log displays a history of snapshots taken or pruned by the Scheduler utility.

Appendices

This chapter details the following:

- **Command Summary – Appendix A, page App-2**
  - **A.1 Menu Commands**
  - **A.2 SANWatch Program Commands**
  - **A.3 Configuration Client Utility Commands**
- **Glossary - Appendix B, page App-7**
- **RAID Levels - Appendix C, page App-13**
  - **C.1 RAID Description**
  - **C.2 Non-RAID Storage**
  - **C.3 RAID 0**
  - **C.4 RAID 1**
  - **C.5 RAID 1(0+1)**
  - **C.6 RAID 3**
  - **C.7 RAID 5**
  - **C.8 RAID 6**
  - **C.9 RAID 10, 30, 50**
- **Additional References - Appendix D, page App-19**
  - **D.1 Java Runtime Environment**
  - **D.2 SANWatch Update Downloads & Upgrading**
  - **D.3 Uninstalling SANWatch**

Appendix A. Command Summary

This appendix describes the commands available in SANWatch Manager. These commands are presented either in each configuration window, as command buttons on pull-down menus, or on pop-up menus triggered by a mouse right-click.

A.1. Menu Commands

This section lists and explains the commands available from the menus in the menu bar.

A.2. SANWatch Program Commands

SANWatch System Menu Commands (Outer-Shell Window)

Command	Description
Open Device	Connects SANWatch Manager to a particular disk array system.
Auto Discovery	Searches the available RAID systems in the specific range on the network.
Exit <X>	Closes the SANWatch Manager application.

SANWatch Language menu Commands (Outer-Shell Window)

Command	Description
English	Opens English version of the online help.
Deutsch	Opens the Deutsch version of the online help.
日本語	Opens the Japanese version of the online help.
Espanol	Opens the Spanish version of the online help.

SANWatch Window Menu Commands (Outer-Shell Window)

Command	Description
Next Window	This command allows you to switch to the display of the next array being connected.
Tile All	This command arranges currently open windows so that they are all visible and occupy an equal part of the SANWatch application window.
Cascade All	This command arranges currently open windows so that one is placed over the other but every window is still visible.
Hide All	This command functions like the minimize caption button.
Close All	This command closes all currently open windows and ends all software connections.

SANWatch Help Menu Commands (Outer-Shell Window)

Command	Description
About <A>	Displays information about the SANWatch Manager program.
What's this?	Produces an interactive arrow mark. By placing the arrow mark over and clicking on a functional menu or push button, the related help content page displays.
Help Topic	Displays the manager's online help.

SANWatch System Menu Commands (Management Window)

Command	Description
Refresh	Refreshes the status display of the current connection in cases when configuration changes are made through a different interface, e.g., via a terminal connection to the same array.
Logout	Closes the currently open window and ends the current session.

SANWatch Action Menu Commands (Management Window)

Command	Description
Array Information	Displays the second-level menu, which provides access to all information windows. Access to the information windows can also be found on the navigation panel.
Maintenance	Displays the second-level menu, which provides access to all maintenance tasks windows. Access to the maintenance task windows can also be found on the navigation panel.
Configuration	Displays the second-level menu, which provides access to all configuration windows. Access to the configuration windows can also be found on the navigation panel.

.

A.3. Configuration Client Utility Commands

File Menu Commands

Command	Description
Add Host	Creates a new entry by entering a Root Agent server IP.
Exit	Closes the Configuration Client application.

Language Selection Commands

Command	Description
English	Opens English version of the online help.
Deutsch	Opens the Deutsch version of the online help.
日本語	Opens the Japanese version of the online help.
Espanol	Opens the Spanish version of the online help.

Help Menu Commands

Command	Description
About	Displays information about the Configuration Client program.

Tool Bar Commands

Command	Description
Open Bookmark File	Opens a previously saved connection view profile. This profile contains information about Root Agent servers and the RAID arrays being managed by a Root Agent.
Save Bookmark File	Saves the current connection view profile onto your system drive. The default file name is “default.npc.”
Connect RootAgent Server	Connects to a Root Agent server, usually the one you chose as a management and on which you installed the Configuration Client utility. However, you may connect to multiple Root Agent servers from a single workstation.
Disconnect RootAgent	Disconnects from a currently connected Root Agent server.
Help Cursor	Helps linking and displaying the associated help topics with a screen element.
Help	Displays SANWatch Manager online help. Details about the Configuration Client utility are also included.

Root Agent Right-click Menu Commands

Command	Description
Add Host	Connects to a Root Agent server, usually the one that you chose as a management and on which you installed the Configuration Client utility. However, you may connect to multiple Root Agent servers from a single workstation.
Delete Host	Deletes a Root Agent entry from the connection view
Disconnect	Disconnects from a currently connected Root Agent server.
Generate Dummy Events	Creates dummy events for testing the notification functions.
Refresh	Refreshes the connection view status. Updates the connection information about Root Agent(s) and the RAID arrays being managed.

This page is intentionally left blank.

Appendix B. Glossary

BBU

Battery backup unit. A BBU protects cached data in the event of power outage.

Fibre

(Also known as "Fibre Channel") A device protocol (in the case of RAID, a data storage device) capable of high data transfer rates. Fibre Channel simplifies data bus sharing and supports greater speed and more devices on the same bus. Fibre Channel can be used over both copper wire and optical cables.

Fiber

An optical network data transmission type of cable, whose initial letter is only capitalized when put at the beginning of a sentence.

HBA

Host-**B**us **A**dapter – an HBA is a device that permits a PC bus to pass data to and receive data from a storage bus (such as SCSI or Fibre Channel).

Host

A computer, typically a server, which uses a RAID system (internal or external) for data storage.

Host LUN

(See Host and LUN). "Host LUN" is another term for a LUN. Host LUNs often apply to the combinations of host channel IDs and the subordinate LUN numbers.

I^2C

Inter-Integrated Circuit – a type of bus designed by Philips Semiconductors, which is used to connect integrated circuits. I^2C is a *multi-master bus*, which means that multiple chips can be connected to the same bus and each one can act as a master by initiating a data transfer. I^2C connect device presence detection circuitry and temperature sensors within EonStor enclosures.

In-Band SCSI

(Also known as "in-band" or "In-band".) A means whereby RAID management software can access a RAID array via the existing host links and SCSI protocols. (Note: the in-band SCSI is typically used in places with no network connections.)

In-band is also implemented with a Fibre Channel host connection.

iSCSI

iSCSI is Internet SCSI (Small Computer System Interface), an Internet Protocol (IP)-based storage networking standard for linking data storage facilities, developed by the Internet Engineering Task Force (IETF).

ISEMS

Infortrend **S**imple **E**nclosure **M**anagement **S**ystem – an I^2C-based enclosure monitoring standard developed by Infortrend Technologies, Inc.

JBOD

Just a **B**unch **o**f **D**isk – non-RAID use of multiple hard disks for data storage.

JRE

Java **R**untime **E**nvironment – the Solaris Java program used to run .JAR applications locally, over a network, or the Internet.

Logical Drive

Typically, a group of hard disks logically combined to form a single large storage volume. Often abbreviated "LD."

Logical Volume

A group of logical drives logically combined to form a single large storage unit. The logical drives contained within a logical volumes are striped together. Often abbreviated "LV."

LUN

Logical **U**nit **N**umber **–** A 3-bit identifier used on a bus to distinguish between up to multiple devices (logical units) with the same host ID.

Mapping

The assignment of a protocol or logical ID to a device for the purposes of presenting a RAID storage volume to an application server and/or device management.

Mirroring

A form of RAID where two or more identical copies of data are kept on separate disks. Used in RAID 1.

Configuration Client

An independently run software application included with SANWatch, which permits centralized management using the Root Agent as the bridging element and event notification via various methods including e-mail and fax.

NRAID

Non-RAID. The capacities of all the drives are combined to become one logical drive (no block striping). In other words, the capacity of the logical drive is the total capacity of the physical drives. NRAID does not provide data redundancy.

Parity

Parity checking is used to detect errors in binary-coded data. The fact that all numbers have parity is commonly used in data communications to ensure the validity of data. This is called parity checking.

Parity in RAID enables fault tolerance by creating a sum of data and saving it across member drives or on a dedicated parity drive.

RAID

Redundant Arrays of Independent Disks (Originally "Redundant Arrays of Inexpensive Disks"). The use of two or more disk drives instead of one disk, which provides better disk performance, error recovery, and fault tolerance, and includes interleaved storage techniques and mirroring of important data.

RAID Agent

The intermediate SANWatch module that communicates between RAID controller firmware and RAIDWatch program. A RAID agent receives SANWatch Manager commands and retrieves information from RAID firmware, such as the event log.

RAID Agent comes embedded with RAID array firmware. RAID Agent can also be manually installed onto a server that is directly-attached with a RAID array and communicates with it using the in-band protocols. See description of in-band.

SANWatch Manager

The SANWatch management software interface.

SAF-TE

SCSI **A**ccessed **F**ault-**T**olerant **E**nclosures – an enclosure monitoring device type used as a simple real-time check on the go/no-go status of enclosure UPS, fans, and other items.

SAN

Storage **A**rea **N**etwork – is a high-speed subnetwork of shared storage devices. A storage device is a machine that contains nothing but a disk or disks for storing data. A SAN's architecture works in a way that makes all storage devices available to all servers on a LAN or WAN. Because stored data does not reside directly on the network's servers, server power is utilized for applications rather than for passing data.

SASL

SASL is the **S**imple **A**uthentication and **S**ecurity **L**ayer, a mechanism for identifying and authenticating a user login to a server and for providing negotiating protection with protocol interactions.

SCSI

Small **C**omputer **S**ystems **I**nterface (pronounced "scuzzy") – a high-speed interface for mass storage that can connect computer devices such as hard drives, CD-ROM drives, floppy drives, and tape drives. A SCSI bus can connect up to sixteen devices.

S.E.S.

SCSI **E**nclosure **S**ervices is a protocol used to manage and sense the state of the power supplies, cooling devices, temperature sensors, individual drives, and other non-SCSI elements installed in a Fibre Channel JBOD enclosure.

S.M.A.R.T.

Self-**M**onitoring, **A**nalysis and **R**eporting **T**echnology – an open standard for developing disk drives and software systems that automatically monitor a disk drive's health and report potential problems. Ideally, this should allow users to take proactive actions to prevent impending disk crashes.

SMS

The **S**hort **M**essage **S**ervice (SMS) is the ability to send and receive text messages to and from mobile telephones. SMS was created and incorporated into the Global System for Mobiles (GSM) digital standard.

Spare

Spares are defined as dedicated (Local), Global, or Enclosure-specific. A Spare is a drive designation used in RAID systems for drives that are not used but are instead "hot-ready" and used to automatically replace a failed drive. RAIDs generally support two types of spare, Local and Global. Local Spares only replace drives that fail in the same logical drive. Global Spares replace any faulty drive in the RAID configuration. An Enclosure spare replaces only a faulty drive within the same enclosure.

Stripe

A contiguous region of disk space. Stripes may be as small as one sector or may be composed of many contiguous sectors.

Striping

Also called RAID 0. A method of distributing data evenly across all drives in an array by concatenating interleaved stripes from each drive.

Stripe Size

(A.k.a. “chunk size.”) The smallest block of data read from or written to a physical drive. Modern hardware implementations let users tune this block to the typical access patterns of the most common system applications.

Stripe Width

The number of physical drives used for a stripe. As a rule, the wider the stripe, the better the performance.

Write-back Cache

Many modern disk controllers have several gigabytes of cache on board. The onboard cache gives the controller greater freedom in scheduling reads and writes to disks attached to the RAID controller. In the write-back mode, the controller reports a write operation as complete as soon as the data is in the cache. This sequence improves write performance at the expense of reliability. Power failures or system crashes on a system without cache protection, e.g., a BBU or UPS, can result in lost data in the cache, possibly corrupting the file system.

Write-through Cache

The opposite of write-back. When running in a write-through mode, the controller will not report a write as complete until it is written to the disk drives. This sequence reduces read/write performance by forcing the controller to suspend an operation while it satisfies the write request.

This page is intentionally left blank.

Appendix C. RAID Levels

This appendix provides a functional description of Redundant Array of Independent Disks (RAID). This includes information about RAID and available RAID levels.

C.1. RAID Description

Redundant Array of Independent Disks (RAID) is a storage technology used to improve the processing capability of storage systems. This technology is designed to provide reliability in disk array systems and to take advantage of the performance gains multiple disks can offer.

RAID comes with a redundancy feature that ensures fault-tolerant, uninterrupted disk storage operations. In the event of a disk failure, disk access will still continue normally with the failure transparent to the host system.

RAID has several different levels and can be configured into multi-levels, such as RAID 10, 30, and 50. RAID levels 1, 3 and 5 are the most commonly used levels, while RAID levels 2 and 4 are rarely implemented. The following sections described in detail each of the commonly used RAID levels.

RAID offers the advantages of Availability, Capacity, and Performance. Choosing the right RAID level and drive failure management can increase data Availability, subsequently increasing system Performance and storage Capacity. Infortrend external RAID controllers provide complete RAID functionality and enhance drive failure management.

C.2. Non-RAID Storage

One common option for expanding disk storage capacity is simply to install multiple disk drives into the system and then combine them end-to-end. This method is called *disk spanning*.

In disk spanning, the total disk capacity is equivalent to the sum of the capacities of all SCSI drives in the combination. This combination appears to the system as a single logical drive. For example, combining four 1GB drives in this way would create a single logical drive with a total disk capacity of 4GB.

Disk spanning is considered non-RAID due to the fact that it provides neither redundancy nor improved performance. Disk spanning is inexpensive, flexible, and easy to implement; however, it does not improve the performance of the drives and any single disk failure will result in total data loss.

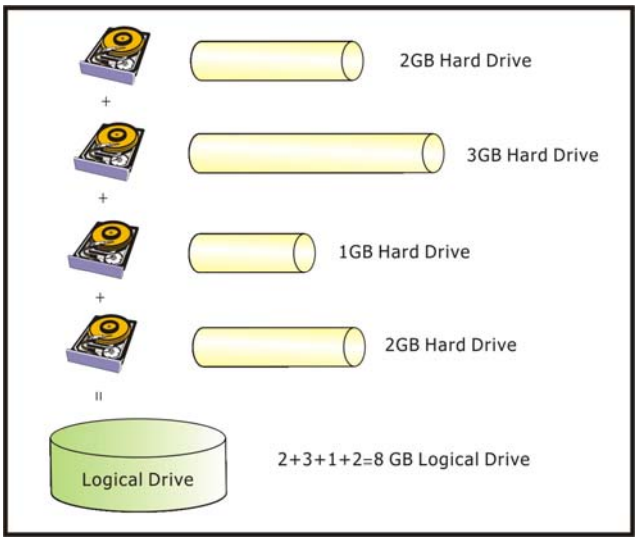


Figure C-1: Non-RAID Storage

C.3. RAID 0

RAID 0 implements *block striping* where data is broken into logical blocks and striped across several drives. Although called RAID 0, this is not a true implementation of RAID because there is no facility for redundancy. In the event of a disk failure, data is lost.

In block striping, the total disk capacity is equivalent to the sum of the capacities of all drives in the array. This combination of drives appears to the system as a single logical drive.

RAID 0 provides the highest performance without redundancy. It is fast because data can be simultaneously transferred to/from multiple disks. Furthermore, read/writes to different drives can be processed concurrently.

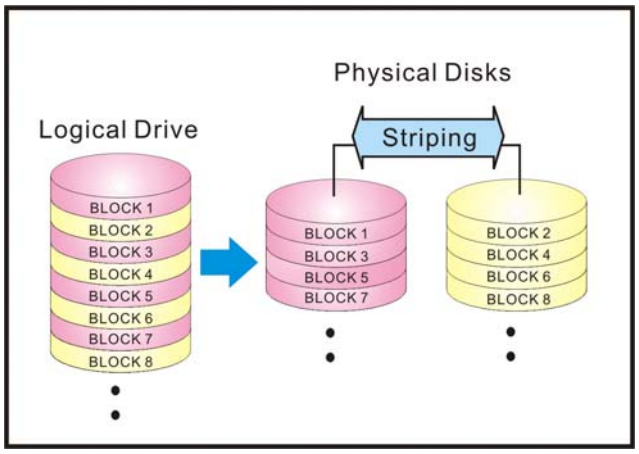


Figure C-2: RAID0 Storage

C.4. RAID 1

RAID 1 implements *disk mirroring* where a copy of the same data is recorded onto two sets of striped drives. By keeping two copies of data on separate disks or arrays, data is protected against a disk failure. If a disk on either side fails at any time, the good disks can provide all of the data needed, thus preventing downtime.

In disk mirroring, the total disk capacity is equivalent to half the sum of the capacities of all drives in the combination. For example, combining four 1GB drives would create a single logical drive with a total disk capacity of 2GB. This combination of drives appears to the system as a single logical drive.

RAID 1 is simple and easy to implement; however, it is more expensive as it doubles the investment required for a non-redundant disk array implementation.

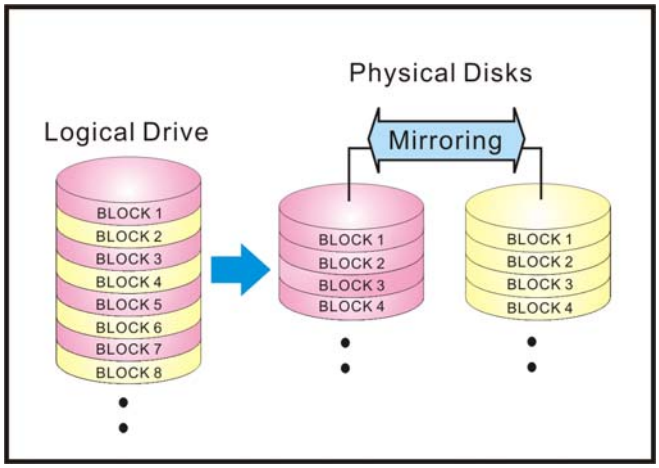


Figure C-3: RAID1 Storage

In addition to the data protection RAID 1 provides, this RAID level also improves performance. In cases where multiple concurrent I/Os are occurring, these I/Os can be distributed between two disk copies, thus reducing total effective data access time.

C.5. RAID 1(0+1)

RAID 1(0+1) combines RAID 0 and RAID 1 – *mirroring and disk striping.* RAID (0+1) allows multiple drive failure because of the full redundancy of the hard disk drives. If more than two hard disk drives are chosen for RAID 1, RAID (0+1) will be performed automatically.

IMPORTANT!

RAID (0+1) will not appear in the list of RAID levels supported by the controller. RAID (0+1) automatically applies when configuring a RAID1 volume consisting of more than two member drives.

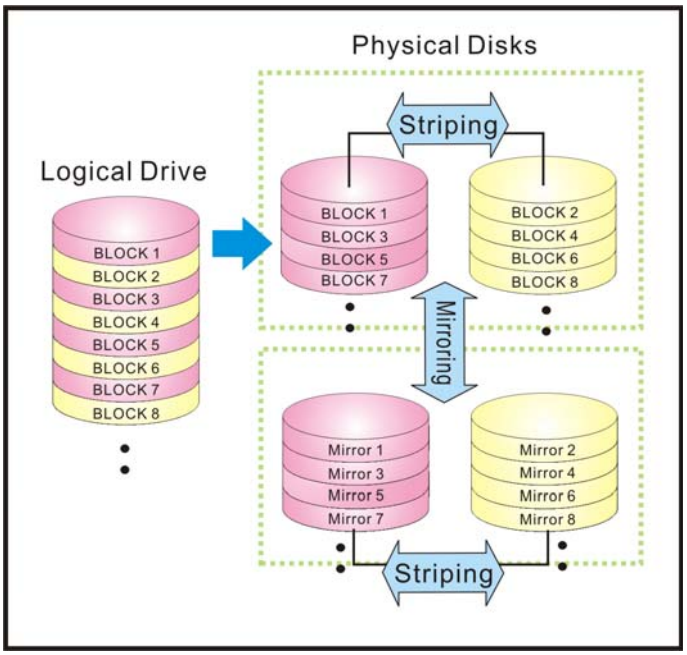


Figure C-4: RAID 1(0+1) Storage

C.6. RAID 3

RAID 3 implements *block striping with dedicated parity*. This RAID level breaks data into logical blocks into the size of a disk block, and then stripes these blocks across several drives. One drive is dedicated to parity. In the event a disk fails, the original data can be reconstructed by XOR calculation from the parity information.

In RAID 3, the total disk capacity is equivalent to the sum of the capacities of all drives in the combination, excluding the parity drive. For example, combining four 1GB drives would create a single logical drive with a total disk capacity of 3GB. This combination appears to the system as a single logical drive.

RAID 3 provides increased data transfer rates when data is being accessed in large chunks or sequentially.

However, in write operations that do not span multiple drives, performance is reduced since the information stored in the parity drive needs to be recalculated and rewritten every time new data is written to any of the data disks.

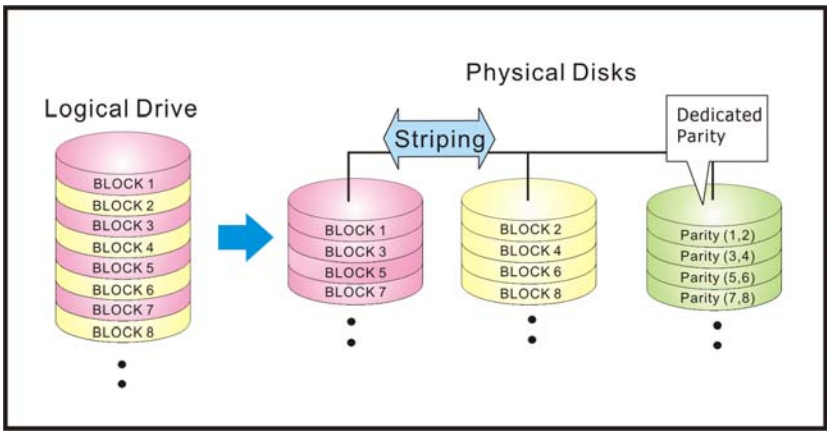


Figure C-5: RAID 3 Storage

C.7. RAID 5

RAID 5 implements *multiple-block striping with distributed parity*. This RAID level offers the same redundancy available in RAID 3, though the parity information is distributed across all disks in the array. Data and relative parity are never stored on the same disk. In the event a disk fails, original data can be reconstructed using the available parity information.

For small I/Os, as few as one disk may be activated for improved access speed.

RAID 5 offers both increased data transfer rates when data is being accessed in large chunks or sequentially and reduced total effective data access time for multiple concurrent I/Os that do not span multiple drives.

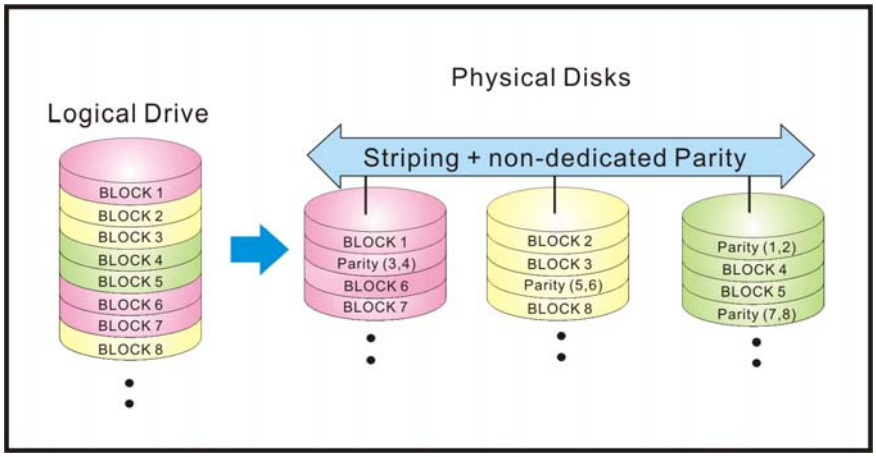


Figure C-6: RAID 5 Storage

C.8. RAID 6

A RAID 6 array is essentially an extension of a RAID 5 array with a second independent distributed parity scheme. Data and parity are striped on a block level across multiple array members, just like in RAID 5, and a second set of parity is calculated and written across all the drives.

The goal of this duplication is solely to improve fault tolerance; RAID 6 can handle the failure of any two drives in the array while other single RAID levels can handle at most one fault. This is a perfect solution when data is mission-critical.

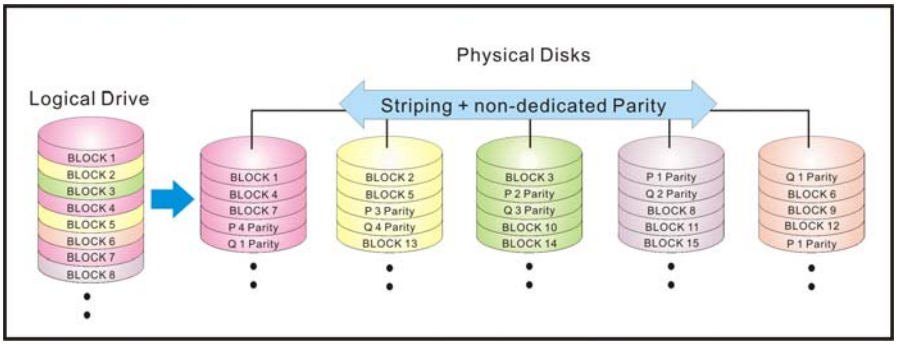


Figure C-7: RAID 6 Storage

C.9. RAID 10, 30, 50 and 60

Infortrend implements RAID 10, 30, 50 and 60 in the form of logical volumes. Each logical volume consists of one or more logical drives. Each member logical drive can be composed of a different RAID level. Members of a logical volume are striped together (RAID 0); therefore, if all members are RAID 3 logical drives, the logical volume can be called a RAID 30 storage configuration.

Using logical volumes to contain multiple logical drives can help manage arrays of large capacity. It is, however, difficult to define the RAID level of a logical volume when it includes members composed of different RAID levels.

Appendix D. Additional References

This appendix provides direction to additional references that may be useful in creating and operating a RAID, and in using SANWatch and SANWatch Manager.

D.1. Java Runtime Environment

JRE (Java Runtime Environment) is a shareware product from Sun/Solaris. Two websites that may be of use relative to JRE are:

The main Java website URL: **java.sun.com**

The JRE download website URL:

www.sun.com/software/solaris/jre/download.html

D.2. SANWatch Update Downloads & Upgrading

Infortrend will provide SANWatch Agent and SANWatch Manager updates periodically both via our ftp server and as new CD releases. Our ftp site can be accessed via our website at:

ftp.infortrend.com.tw

D.3. Uninstalling SANWatch

SANWatch agents, Configuration Client and SANWatch Manager can be uninstalled. Choose the Uninstall icon in the SANWatch group. Click on the Uninstall button on the bottom of the uninstallation program window to start the uninstall process. The SANWatch program will be uninstalled and files will be removed from your computer.

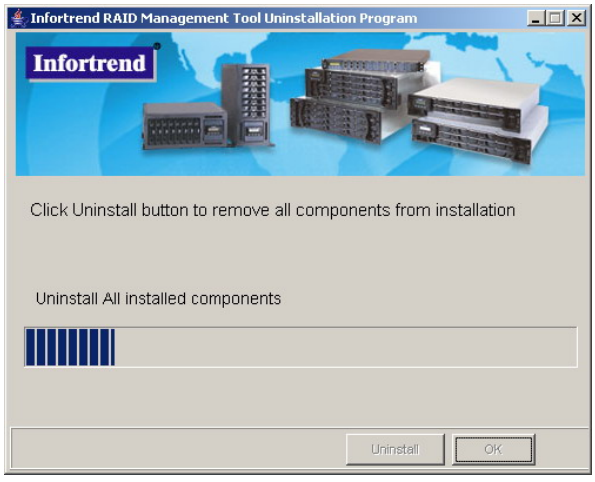


Figure D-1: SANWatch Uninstallation Program

This page is intentionally left blank.